INQUIRY: The Journal of Health Care Organization, Provision, and Financing
Volume 54: 1–12

DOI: 10.1177/0046958017711759
journals.sagepub.com/home/inq
SAGE

Compliance With Electronic Medical Records Privacy Policy: An Empirical Investigation of Hospital Information Technology Staff

Ming-Ling Sher, MPH[1], Paul C. Talley, PhD[2], Ching-Wen Yang, PhD[3], and Kuang-Ming Kuo, PhD[2]

Abstract

The employment of Electronic Medical Records is expected to better enhance health care quality and to relieve increased financial pressure. Electronic Medical Records are, however, potentially vulnerable to security breaches that may result in a rise of patients' privacy concerns. The purpose of our study was to explore the factors that motivate hospital information technology staff's compliance with Electronic Medical Records privacy policy from the theoretical lenses of protection motivation theory and the theory of reasoned action. The study collected data using survey methodology. A total of 310 responses from information technology staff of 7 medical centers in Taiwan was analyzed using the Structural Equation Modeling technique. The results revealed that perceived vulnerability and perceived severity of threats from Electronic Medical Records breaches may be used to predict the information technology staff's fear arousal level. And factors including fear arousal, response efficacy, self-efficacy, and subjective norm, in their turn, significantly predicted IT staff's behavioral intention to comply with privacy policy. Response cost was not found to have any relationship with behavioral intention. Based on the findings, we suggest that hospitals could plan and design effective strategies such as initiating privacy-protection awareness and skills training programs to improve information technology staff member's adherence to privacy policy. Furthermore, enhancing the privacy-protection climate in hospitals is also a viable means to the end. Further practical and research implications are also discussed.

Keywords

compliance, electronic medical records, personal health records, privacy policy, protection motivation theory, theory of reasoned action

Introduction

To improve health care quality and to ease increased financial pressure, it is widely acknowledged that the health care industry should extensively leverage health information technologies (IT) to overcome such challenges.[1-3] One assumed method to meet these initiatives is through the adoption of Electronic Medical Records (EMR) systems.[4] Generally, EMR refers to a collection of software applications commonly utilized to communicate orders for medical care, record related facts concerning a patient's medical history, and to circulate results of laboratory testing.[5] Via EMR, health care professionals can access patient information instantly without the set limitations of time and location.[3] More important, they may acquire support to improve the quality of clinical decision-making.[3] Along with the development of more comprehensive EMR, a highly increased volume of medical records will become easily accessible to both authorized and unauthorized users both inside and outside the health care facilities.[6] EMR are, thus, potentially vulnerable to security breaches that may result in a rise of patients' privacy concerns.[7] This issue needs special attention due to the fact that EMR adoptions are currently widespread, and they have been well acknowledged as a cost-effective investment tool.[8-10] It is, thus, an important mandate for hospitals to effectively secure the privacy of EMR to diminish their patients' overall privacy concerns. The literature has further asserted that the reason why security breaches continue to occur in most organizations is due to administrative employees remaining as one

[1]National Chung Cheng University, Chiayi, Taiwan (R.O.C.)
[2]I-Shou University, Kaohsiung City, Taiwan (R.O.C.)
[3]Taichung Veterans General Hospitals, Taichung City, Taiwan (R.O.C.)

Received 30 August 2016; revised 12 February 2017; revised manuscript accepted 27 April 2017

Corresponding Author:
Kuang-Ming Kuo, Department of Healthcare Administration, I-Shou University, No. 8, Yida Road, Yanchao District, Kaohsiung City 82445, Taiwan (R.O.C.).
Email: kuangmingkuo@gmail.com

of the primary sources of threat.[11,12] Specifically, most violations of patient privacy in medical facilities result from staff abuse or misuse of the right to access patient records[13,14]; even so, medical facilities are legally bound and ethically obligated to protect the privacy of EMR regardless of the existence of any internal regulations. Many countries, including Taiwan, have even externally regulated hospitals to ensure the relative safety of EMR.[14,15] Furthermore, any noncompliance with those privacy rules may involve both civil money and criminal penalties. For example, in the United States, the amount of civil monetary penalty is US$100 to US$50 000 or more per violation, and the criminal penalty may result in a fine of US$250 000 and up to 10 years of imprisonment.[14] In Taiwan, the maximum civil monetary penalty can result in a payment of more than US$6 million and 5 years of imprisonment.[16] Hospitals' employees are thus wholly mandated to protect the privacy of EMR; nevertheless, they may still not act as preregulated.[13,14] Hence, all hospital employees who have EMR access privileges are still to be considered as possible threats to EMR privacy, in addition to those intrusive individuals who are outside the system domain.

Previous privacy-related studies in an EMR context can be roughly classified into three major categories: (1) technical solutions to avoid or secure privacy problems in EMR, (2) patients' privacy concerns and responses regarding EMR, and (3) privacy-protection from a law perspective. In the first type of study, the primary objective is to propose a sound mechanism or an optimal algorithm useful to secure expected EMR privacy.[17-20] The second type of study focuses on exploring the privacy concerns of patients/health care professionals and/or the results of such privacy concerns throughout the EMR process.[7,21-24] The last type of literature emphasizes the potential limitation of privacy law and how to respond to such limitation from a legal perspective.[25,26]

By reviewing privacy-related studies in an EMR context, we have obtained a deeper understanding of how to technically and lawfully design EMR that affords better characteristics that preserve data integrity and also address patients' concerns related to general EMR privacy constraints. However, the nature of how hospitals can effectively secure the privacy of EMR through "other-than-technical" solutions seems to have been insufficiently investigated to date. Literature, indeed, has begun pointing out the relative importance of employee compliance to organizational rules, or set policies and procedures, which may provide a useful mechanism in modeling employees' proper attitudes or behaviors concerning how organizational resources should be used.[11-13,27] However, results often reveal that employees do not choose to adhere to such rules or policies as a matter of course. Further, little study has specifically been focused on IT staff in hospitals, who are the administrators of and have full control of EMR systems. More important, IT staff knowledge of how users protect EMR privacy is found to mismatch how users really operate in practice.[28] Consequently, the perceptions of IT staff toward the privacy of EMR should be carefully investigated. The privacy policy of EMR refers to a formal statement articulating the privacy rules of the hospital and concerns to all employees who have access to EMR and such related information assets.[29] Any adherence to stated EMR policy by IT staff is always a matter of interest to their employer.

The primary purpose of our study was to investigate the factors that effectively motivate, rather than coerce, hospital IT staff's compliance with a stated EMR privacy policy. We proposed a research model on a basis of well-recognized and fitting theories. More specifically, we drew upon the literature of protection motivation theory (PMT)[30,31] and theory of reasoned action (TRA)[32] to investigate IT staff perceptions regarding their widespread compliance with EMR privacy policy in a health care setting. Previous literature[33] of systematic review suggests that behavioral science theories such as PMT used to explain individuals' choices as to whether or not to apply specific protective measures regarding possible threats,[30,31] and TRA may be used to predict individuals' behaviors[32] for investigating policy-compliance behaviors.

Research Model and Research Hypotheses

Conceptual Model Formulation

To capture the essence of IT staff's compliance intention of EMR privacy policy, we integrated PMT[30,31] and TRA[32] to form our theoretical underpinning. First, the PMT explains how delineating an individual's protection motivation can be aroused through his or her appraisal mechanisms whenever confronting a threat, which seems suitable for explaining how IT staff can avert the potential threat of EMR breaches. The PMT postulates that protection motivation is the result of two cognitive mediating processes, namely, threat appraisal (referring to the assessment of the probability of and severity of a threat), and coping appraisal (meaning the assessment of one's ability to cope with and to avert the threat).[30,31] Furthermore, fear arousal, which assesses how much fear the threat evokes for an individual,[34] is an emotional response to threat appraisal[34-36] and, in its turn, influences an individual to undertake protective behaviors.[34] An individual may, however, decide not to take such protective behaviors.[33] And such a dichotomous decision is precisely why there is a compliance of EMR privacy policy in place, which makes the PMT an appropriate theoretical underpinning for our study. Second, the TRA illustrates that an individual's behavior intention is directed by his or her attitude, and the attitude is a function of an individual's beliefs, and can thereby predict IT staff's policy-compliance intention. Beliefs, or cognitions, represent the information he or she has about an object, issue, or event while attitude, or affect, refers to a person's feelings toward and assessment of some objects, issues, or events.[32] Furthermore, a person's intention is also a function of certain beliefs.[32] Accompanying TRA,

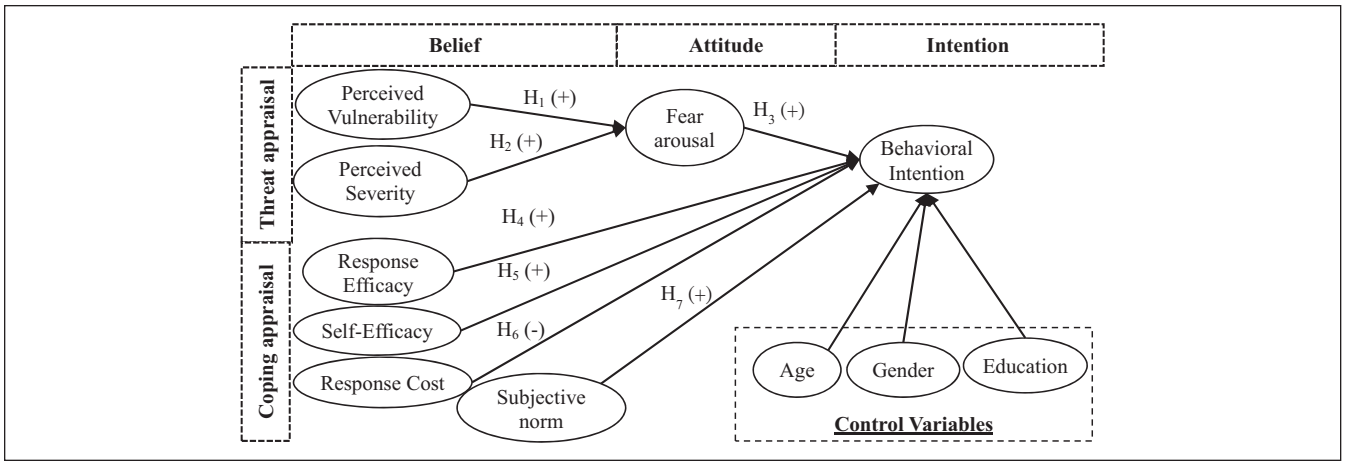

Figure 1. Research model.

PMT can, thus, be regarded as a more comprehensive model for predicting protective behavioral intentions.[33]

In our study context, any EMR breaches may be considered as a perceptible threat to both hospitals and health care employees, including IT staff, because such an event would negatively infringe on a hospital's positive reputation and even with its profit-driven business climate. In just such a situation, the IT staff may, thus, stand to lose their jobs or even suffer legal ramifications if they were somehow connected to possible EMR breaches, rightfully or wrongfully. In facing such conflictive situations, IT staffers have to elect to cope with the perceived threat (ie, in full or partial accordance with the stated EMR privacy policy) or not choose to cope with the threat at all. In other words, IT staff will undergo the threat appraisal process. An emotional feeling of fear may then be aroused after evaluating a potential threat and the level of severity the potential EMR breaches may pose. Besides the support of PMT, such a presumed relationship between threat appraisal and fear arousal can further be evidenced from the manner in which an individual's belief (threat appraisal) can predict his or her attitude (fear arousal, an emotional response), as articulated by the TRA.[32] The IT staff member will then generate his or her behavioral intention to comply with a given privacy policy through direct action or affirmation.

Furthermore, they may also evaluate the efficacy of, or their ability to comply with, the cost of compliance to a given privacy policy, and a behavioral change (ie, protection motivation) regarding which coping responses will then occur according to PMT.[30] Furthermore, such compliance intention can also be determined by adherence to a subjective norm as posited by TRA.[32] Finally, we include three control variables in the proposed model, namely, those of age, gender, and the education of respondents to eliminate those unknown influences.[36,37] Figure 1 shows our research model integrative of both PMT and TRA.

Research Hypotheses

The relationships of perceived vulnerability and perceived severity with fear arousal. In our study, perceived vulnerability refers to the IT staff member's probability assessment of a threat resulting from noncompliance with EMR privacy policy, while perceived severity pertains to the understood consequences of a threat originating from noncompliance with privacy policy.[38] Fear arousal refers to the extent to which IT staff members are concerned with EMR being threatened.[39] In line with PMT, perceived vulnerability and perceived severity can trigger an individual's protection motivation to manifest.[30,31] In an EMR privacy setting, these threats can be conceived of as the IT staff's appraisal of the probability of exposure to and the consequences stemming from an EMR privacy threat. Furthermore, we favored the assertion by Tanner et al[36] that the state of fear (eg, conceptualized as fear arousal in our study) is assumed to be aroused after assessing the vulnerability and severity of any threat. In other words, fear arousal may mediate an individual's threat appraisal and protection motivation to a threat. Applying such a rationale to our study, if the IT staff perceive that the EMR privacy may be violated after assessing the probability of and severity of the occurrence of an EMR privacy threat, IT staff members may become concerned that the injury posited by the threat is substantiated because such a threat may negatively influence the hospital's reputation, business climate, and even personal work settings. In their study of juveniles' response to health hazards typically associated with smoking, Arthur and Quester[40] found that juveniles' perceived vulnerability to, along with a perceived notion of severity of, health hazards has a significant and positive relationship with fear. Furthermore, Boss et al[35] also reported that information system users' perceived threat vulnerability and perceived threat severity significantly and positively associated with their fear of possible negative results due to unsafe security behaviors. Thus, the present study hypothesizes the following:

Hypothesis 1 (H1): There is a positive relationship between perceived vulnerability and fear arousal of EMR threat by the IT staff.
Hypothesis 2 (H2): There is a positive relationship between perceived severity and fear arousal of EMR threat by the IT staff.

The relationships of fear arousal, response efficacy, self-efficacy, response cost, and subjective norm with behavioral intention. In their study of online users' intention to use strong passwords, Zhang and McDowell[41] found that fear arousal will change online users' behavior consistently. Furthermore, fear has also been characterized as an emotional state.[30] According to TRA, an individual's attitude (ie, one kind of feeling) can predict his or her behavioral intention.[32] Consequently, if IT staff members reveal a higher level of fear concerning the perceived threat of EMR breaches, they are supposed to become much likelier to comply with a specified privacy policy. Furthermore, they will hold a positive attitude/intention toward individual compliance with a privacy policy to avert any perceived threat. Prior literature[40] also confirmed that juveniles' fear of health hazards associated with smoking significantly predicts the nature of their protective behaviors. Boss et al[35] found that information system users' fear of possible negative results due to unsafe security behaviors is significantly associated with their protective motivation. Thus, the third hypothesis postulates the following:

Hypothesis 3 (H3): Fear arousal will have a positive relationship with the IT staff's behavioral intention to comply with EMR privacy policy.

In addition, according to PMT, coping appraisal is composed of response efficacy, self-efficacy, and response cost. In our study, response efficacy refers to IT staff's compliance with a privacy policy as being a useful means for diminishing the threat of EMR breaches, while self-efficacy is used to measure IT staff member's judgment of himself or herself to be capable of compliance with privacy policy. Response cost is defined as IT staff member's perceived cost of complying with privacy policy and may be inclusive of the money, time, or personal effort involved. Logically, if IT staffers perceive that compliance with privacy policy can effectively avert the threat of EMR breaches, and he or she is confident of adherence to privacy policy, they are more likely to possess a positive attitude/intention toward that given privacy policy. Furthermore, if they consider themselves as being incapable of compliance with a privacy policy due to inherently complicated procedures, or if the compliance behavior requires inordinate amounts of time and effort, they may, thus, be unlikely to adhere to the given privacy policy. Prior studies[42,43] found that response efficacy and self-efficacy positively and significantly predict government employees' compliance with protective strategies concerning information security. Herath and Rao[39] also reported that response cost correlated negatively with employees' attitudes toward security policy. Boss et al[35] and Ifinedo[38] both found that response efficacy and self-efficacy significantly and positively linked with information system users' safe security behavioral intentions, respectively. Boss et al[35] further confirmed that response cost negatively related with information system users' safe security behavioral intentions. According to the above discussion, we postulate the following hypotheses:

Hypothesis 4 (H4): Response efficacy will have a positive relationship with IT staff's behavioral intention to comply with EMR privacy policy.
Hypothesis 5 (H5): Self-efficacy will have a positive relationship with IT staff's behavioral intention to comply with EMR privacy policy.
Hypothesis 6 (H6): Response cost will have a negative relationship with IT staff's behavioral intention to comply with EMR privacy policy.

In our study, subjective norm refers to the IT staff's subjective beliefs about the extent of disapproval for nonadherence to EMR privacy policy among those members who are of paramount importance to the IT staff. According to TRA, an individual's intention toward a specific behavior can be collectively predicted by his or her attitude toward that behavior and subjective norm posed by important others. Hence, if IT staff members hold affirmative feelings toward personal compliance with a privacy policy, and other considered-important people (ie, top management or esteemed colleagues) also think that the IT staff should obey the privacy policy, IT staff members may then be more likely to support the privacy policy of the EMR. In several studies of organizational security behavior, subjective norm has consistently been a significant predictor of one's intention to comply with security policy.[38-39,44] Based upon the previous discussion, this study, therefore, states the following hypothesis:

Hypothesis 7 (H7): Subjective norm will have a positive relationship with the IT staff's behavioral intention to comply with EMR privacy policy.

Methods

Measures

This research followed Churchill's[45] approach for generating questionnaires, with the research constructs reflectively measured using previously validated instruments.[38,39] We adopted reflective measurements for the following reasons: (1) the indicators are manifestations of the construct, (2) removing an indicator does not alter the conceptual domain of the construct, and (3) indicators can be interchangeable. These characteristics are, therefore, more demonstrative of a reflective construct.[46]

The instruments for perceived vulnerability utilized four items and were adapted from Ifinedo.[38] The perceived severity and fear arousal constructs were measured by using two items, respectively, and they are to be found in Herath and Rao.[39] Response efficacy and self-efficacy were measured by using three items, respectively, and they were also adapted from Herath and Rao.[39] We measured response cost by using two items adapted from Ifinedo.[38] Subjective norm and intention to comply were measured by using four items and three items, respectively, and they were adapted from Herath and Rao.[39] Excluding demographic questions, all items were based on a 7-point Likert-type scale (eg, 1 = *strongly disagree*, and 7 = *strongly agree*).

A pretest, a preliminary trial of the instrument used to ensure that there are no unexpected difficulties before formal investigation,[47] was conducted to establish the scales via a convenience sampling of 10 IT staff members belonging to a major medical center. Based upon subsequent feedback, modification of words and phrases was made to items resulting in a final scale (see Appendix A), which was justified for further testing.

Sample and Data Collection

Permission from the Institutional Review Board of a large hospital in Taiwan was obtained prior to investigation. In Taiwan, medical centers are assumed to be the most sophisticated in their implementation of EMR vis-à-vis other types of medical facilities (eg, regional and district hospitals). Furthermore, Taiwanese hospitals that have adopted EMRs are mandated to formulate policies or rules that can secure the privacy of EMRs according to the governmental regulation, and the hospitals should inform their staff with these policies or rules.[15] Our study's purpose was to explore the determinants of hospital IT staff compliance with EMR privacy policy. Participants within the study must have been granted access to EMR at some point in time. Hence, our primary participants will be the IT staff of these medical centers as they usually have EMR access privileges for at least maintenance purposes. Prior to the administration of the questionnaires, we successfully contacted 7 medical centers to secure their collaboration. We assigned a coordinator for each hospital to help with the distribution and collection of the questionnaires. IT staff in the seven hospitals, including the managerial-level staff who are also IT literate, were invited to participate in a paper-and-pencil survey. A total of 350 questionnaires were distributed to these coordinators according to their respective numbers of IT staff in these 7 hospitals, and a total of 320 questionnaires were returned to the researchers. Excluding 10 incomplete questionnaires, 310 usable questionnaires were left for subsequent analysis.

Results

Descriptive Statistics

Of the 310 valid responses, 62.3% of responses were from male respondents, and 37.7% were from female respondents. Nearly 77.4% of the total respondents were 30 to 49 years of age. Furthermore, the majority of respondents were university educated or graduate school educated (90.0%). Programmers made up the largest group of respondents (41.0%), and more than 48.1% of respondents reported having more than 10 years of prior work experience within the health care industry. Furthermore, all respondents were said to understand relevant EMR privacy policy, with 32.6% of respondents being not very clear about the detailed contents of the codified policy as it might exist. Details of the respondents are shown in Table 1.

Structural Equation Modeling

We first employed a Kolmogorov-Smirnov test to check for the normality of collected data, and the results showed nonnormal distribution ($P < .001$) to some extent. We, therefore, adopted partial least squares (PLS), which is a method that makes no distribution assumption,[48] to analyze the collected data. We used R software,[49] with the semPLS package,[50] to inspect both the measurement model and the structural model of PLS, respectively.[48]

Measurement model. The measurement model in PLS is usually assessed according to three tests: reliability, convergent validity, and discriminant validity.[48,51] Reliability can be evaluated via composite reliability (CR).[48,51] In our study, the CR values of all constructs (see Table 2) were above the threshold of 0.7,[48] indicating sufficient reliability (see Table 2). Although the CR values of the four constructs (ie, perceived vulnerability, perceived severity, subjective norm, and behavioral intention to comply) were all higher than 0.95, they may still indicate an invalid measure of a construct, and it is usually caused by using redundant items.[45] However, the items used in our study were semantically different and, as such, tapped into different aspects of the constructs (see Appendix A), so they were still highly correlated. Furthermore, other literature[52] regards a reliability of 0.95 as a desired standard. Hence, this may imply the measurement model remains valid. For convergent validity, all items in our study had outer loadings >0.7 on their posited factors and loaded highly on the posited factors, suggesting sufficient convergent validity on the indicator level.[48] Fornell and Larcker[51] further suggested that the value of average variance extracted (AVE) of at least 0.5 demonstrates sufficient convergent validity of each construct. As per this criterion, the constructs used in this study demonstrated sufficient convergent validity (see Table 2). Because the factor loadings of perceived severity and behavioral intention to comply were higher than 0.95, we further checked for a collinearity problem. The results revealed that the tolerance value of each construct ranges from 0.24 to 0.81, indicating that collinearity should not be an issue in our study.[53] Furthermore, the inter-construct correlations matrix (see Table 3) exhibited that the square root of AVE for each construct was larger than

Table 1. Descriptive Statistics of Respondents' Characteristics.

Profile	Items	Frequency	Percentage (%)
Gender	Male	193	62.3
	Female	117	37.7
Age	20-29	38	12.3
	30-49	240	77.4
	50-64	32	10.3
Education	High school	4	1.3
	College	27	8.7
	University	158	51.0
	Graduate school	121	39.0
Title	Managerial level	27	8.7
	System analyst	28	9.0
	System designer	16	5.2
	Programmer	127	41.0
	Hardware/Database/Network administrator/Others	112	36.1
Experiences in health care industry (years)	1-3	77	24.8
	4-6	51	16.5
	7-9	33	10.6
	≥10	149	48.1
Understand EMR privacy policy?	Yes	209	67.4
	Yes, but not very clear	101	32.6

Note. EMR = Electronic Medical Records.

Table 2. Reliability and Validity.

Constructs[Source]	No. of items	Factor loading	*M*	*SD*	CR	AVE
Perceived vulnerability[37]	4	0.87-0.93	6.17	0.85	0.95	0.81
Perceived severity[38]	2	0.96	5.35	1.32	0.96	0.93
Fear arousal[38]	2	0.85-0.88	6.07	0.84	0.85	0.74
Response efficacy[38]	3	0.88-0.94	6.16	0.82	0.94	0.83
Self-efficacy[38]	3	0.86-0.93	5.87	0.91	0.92	0.80
Response cost[37]	2	0.87-0.93	5.74	0.93	0.90	0.81
Subjective norm[38]	4	0.90-0.95	6.02	0.86	0.96	0.84
Behavioral intention to comply[38]	3	0.95-0.97	6.10	0.80	0.97	0.92

Note. CR = composite reliability; AVE = average variance extracted.

the correlation of the specific construct with any other constructs in the model, thus indicating the occurrence of adequate discriminant validity.[51]

Structural model. Regarding the assessment of the structural model, the 7 proposed hypotheses were all supported, with the exception of H6 (Response cost → behavioral intention). Overall, the model explained about 45% and 76% of the determined variance in the fear arousal and behavioral intention, respectively. Furthermore, the effects of the three control variables (ie, age, gender, and level of education) were also tested, along with the hypotheses. The results indicated that no one control variable possessed a significant effect on intention, and the results regarding the hypotheses remain unchanged with, or without, these control variables being present. We then assessed the structural model with three key criteria, namely, the predictive relevance Q^2, the f^2, and the q^2 effect size.[48] The Q^2 values for fear arousal and behavioral intention were 0.34 and 0.70, respectively, indicating the structural model had predictive relevance for both constructs.[48] Furthermore, the relationship between perceived vulnerability and fear arousal had a large effect size (f^2 = 0.57) and a large predictive relevance ($q2 = 0.35$), while perceived severity had a small effect size ($f^2 = 0.06$) and a small predictive relevance ($q^2 = 0.04$).[48] Regarding the relationship with behavioral intention, only subjective norm had a medium effect size ($f^2 = 0.26$) and a medium predictive relevance ($q^2 = 0.20$) while other predictor constructs had small effect sizes and small predictive relevance (see Appendix B). Furthermore, as there is no overall fit index in PLS path

Table 3. Correlations Among Constructs.

Constructs	A	B	C	D	E	F	G	H
Fear arousal (A)	**0.90**							
Intention to comply (B)	0.31	**0.96**						
Perceived severity (C)	0.65	0.37	**0.86**					
Perceived vulnerability (D)	0.70	0.29	0.75	**0.91**				
Response cost (E)	0.65	0.23	0.65	0.75	**0.89**			
Response efficacy (F)	0.44	0.32	0.45	0.55	0.55	**0.90**		
Self-efficacy (G)	0.62	0.23	0.64	0.73	0.70	0.53	**0.92**	
Subjective norm (H)	0.68	0.26	0.68	0.77	0.77	0.49	0.80	**0.96**

Note. Diagonal elements show the square root of average variance extracted (AVE).

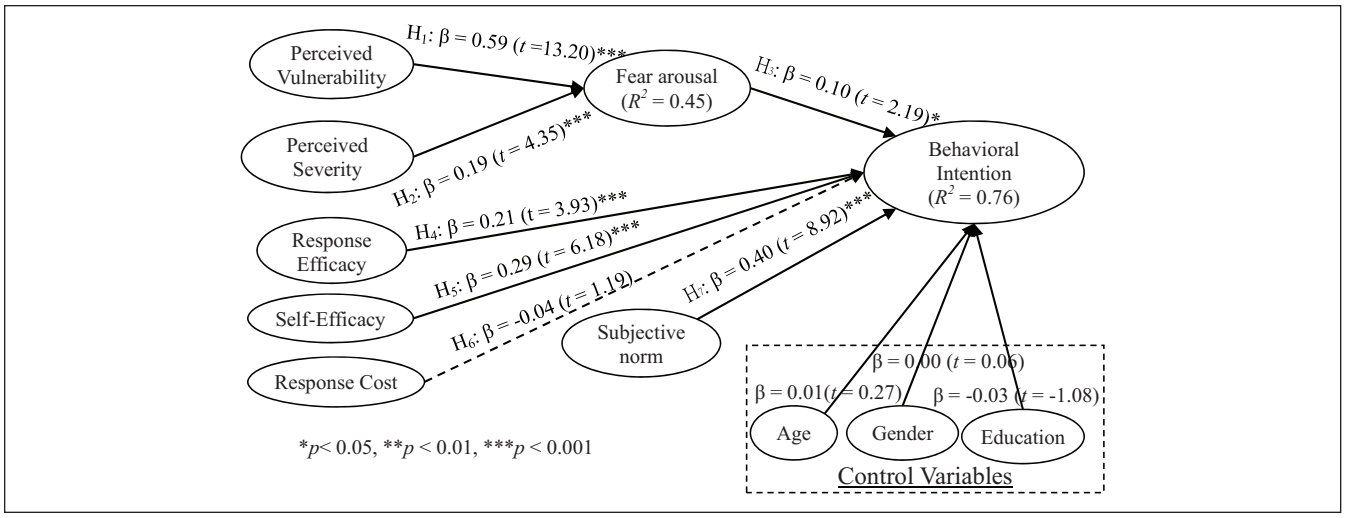

Figure 2. Structural model results.

modeling,[54] we used the global fit measure (GoF), appropriate for reflective measurement modelling,[54] to assess the PLS model.[55] The resulting GoF = 0.71, which surpassed the 0.36 standard for large effect sizes, implied that our model was valid. Figure 2 demonstrated the structural model results.

A Comparison of Differing Models for Predicting Organizational Policy Compliance

Several prior studies[33,38,39,56-59] have also researched employee's compliance of organizational policy from differing theoretical perspectives such as protection motivation theory, theory of planned behavior, deterrence theory, principal agency theory, social cognitive theory, social bond theory, control theory, regulatory focus theory, and reactance theory. The findings of these studies have absolutely added to the knowledge of organizational policy compliance. In general, the variances explained by these models range from 30% to 70% (see Appendix C). Among these models, protection motivation theory and theory of planned behavior are most used to predict employee's behavioral intention, and usually have a good explanatory power than other models. For example, Ifinedo[38] combined protection motivation and theory of planned behavior to predict information system security compliance and is the only study that explained it is comparatively large (R^2 = 70%). Our study integrated protection motivation theory and theory of reasoned action to examine hospital IT staff's intention to comply with EMR privacy policy and also explained about 76% of the variance of behavioral intention. The reason why PMT has such a high variance explanatory power might be due to the fact that PMT fits well with our study context, because PMT was originally proposed to demonstrate how an individual may cope with a potential threat, which are the EMR breaches in our study.

Discussion

In line with the assertion of PMT, we found that perceived vulnerability and perceived severity significantly and positively correlated with fear arousal, respectively. The result matches those observed in prior studies of differing disciplines.[39,40] Ifinedo[38] also found that perceived vulnerability significantly predicted security policy compliance intention

of employees. Similar to perceived vulnerability, if the IT staff considers EMR breaches to be a serious threat, not only to the hospitals but also to themselves, they may fear that such a threat might endanger the hospital's profitability and also the security of the workplace. This finding supports previous literature.[40] Other studies also confirmed the link between perceived severity and individuals' behavioral intention.[38,43] Hence, both perceived vulnerability to and perceived severity of the threat of EMR breaches jointly arouse IT staff's fear, while perceived vulnerability had a stronger relationship with fear arousal than that of perceived severity.

We also found that fear arousal was a significant predictor of behavioral intention. The more IT staff members are concerned with the threat of EMR breaches, the more they will hold an increased positive intention toward privacy policy. This finding is in line with the study of Zhang and McDowell.[41] Herath and Rao[39] also found that the concern level (akin to fear arousal in our study) of employees significantly predicts their attitude toward security policy. Further, response efficacy was also a strong determinant of behavioral intention. If the IT staff believes that privacy policy is an effective countermeasure in dealing with the threat of EMR breaches, the more likely they will be to comply with existing organizational privacy policy. This also accords with earlier observations.[38,43] Regarding the relationship between self-efficacy and behavioral intention, the results of structural model analysis supported that an increased confidence to comply with privacy policy perceived by the IT staff can improve their intention toward compliance with privacy policy. The findings are in line with earlier studies.[39,42,43] However, the findings of the relationship between response cost and behavioral intention do not support the previous research[39,43] but were in line with the results of Ifinedo.[38] One possible reason for the insignificant results arrived at might be that IT staff understand that whoever uses EMR will be fully logged-in and, therefore, visible to system administration. Any illegal attempts could be interdicted, so IT staff will, thus, adhere to privacy policy at any cost and might not view the cost to protect the privacy as an issue of particular importance or of personal interest. Moreover, as the original TRA states, an individual's behavioral intention can be determined through a subjective norm. Our findings also corroborate the notions of TRA and other studies.[38,39] Several implications for the literature and for practice can be drawn from the findings comprised in our study.

Academic Implications

For academics, our study aids in the accumulation of knowledge related to the issue of compliance with a privacy policy in an EMR context. This study further empirically validated the appropriateness of integrating PMT originated from the health domain and TRA from the psychology discipline to address IT staff's adherence to a given privacy policy. To the best of our knowledge, there is little extant study accomplished to explore privacy policy issues based on the tandem PMT and TRA aspects. By incorporating the intention construct adapted from TRA, the concept of protection motivation can be more clearly expressed than in the original PMT. Furthermore, PMT can be made more useful by the inclusion of other social norms such as with the subjective norm, which is also adapted from TRA. The result showed that the combination of the two theories allows for a better understanding of the determinants that motivate IT staff to comply with a privacy policy related to EMR. Future research may further refine our proposed model to better predict other hospital employees' compliance with an institutional privacy policy. Further, our study revealed that perceived vulnerability and perceived severity can stir IT staff's fear regarding the threat of EMR breaches, and fear arousal mediates with intention to form an adherence toward a privacy policy. Future studies may be used to explore the role that fear arousal plays in those relationships that are in conjunction with perceived vulnerability, perceived severity, and protection motivation to obtain improved understanding.

Practical Implications

There are also several practical implications that may be derived from our study. First, the support of fear arousal may imply that hospitals can initiate EMR privacy-protection awareness programs to elicit an IT staff member's sense of possible deleterious consequences resulting from the threat of EMR breaches. These privacy-protection awareness programs may be concentrated on the belief that vulnerability to, and the severity of, negative consequences are directly related to the threat of EMR breaches. A stronger emphasis can be placed on the direct probability of EMR breaches because perceived vulnerability had the highest influence on fear arousal. IT staff members may, thus, undergo a rational bout of emotional fear, which can in turn realize adherence to privacy policy to diminish the perceived threat. Furthermore, an overriding support of response efficacy may demonstrate that the above-mentioned privacy-protection awareness programs have the marked ability to educate the IT staff to the purpose, and as to the effects of, privacy policy implementation. This demonstration can help the IT staff understand the significant benefits of a privacy policy and exactly how such a privacy policy can settle the threat of possible EMR breaches. The significant result of self-efficacy may also imply that these privacy-protection awareness programs have the potential to equip individuals with sufficient knowledge, skills, or tools requisite for compliance with a stated privacy policy. Both the implications for response efficacy and self-efficacy can convince IT staff members to have positive feelings regarding any personal adherence to privacy policy. With exhibited positive attitude, IT staff are more likely to comply with a privacy policy specifically geared to EMR. Our results further demonstrate that subjective norm affects IT staff's intention to adhere to privacy policy. Hence, managers can improve IT staff's compliance intention by enhancing the relative privacy climate in hospitals and

encouraging colleagues to advocate compliance with a privacy policy for EMR, as IT staff's compliance intention can be motivated by the opinions of supervisory staff, colleagues, and also the general staff of both small-scale and large-scale medical record departments.

Limitations

Several common limitations may exist in this study. First, the sample is drawn from only 7 medical centers in Taiwan, and it does not comprise a more representative sampling. Consequently, inferences to the larger population cannot be safely made. Furthermore, the survey conducted in this study was based on self-reporting rather than through observation or through the recording of participants' routine behavioral patterns. We did not investigate the actual compliance behavior of IT staff as it might occur. Future research can, thus, investigate the issue to better elucidate the relationships among these reported constructs.

Conclusions

By integrating PMT and TRA, our study proposed and then empirically validated a model to investigate compliance with EMR privacy policies among hospital IT staff members. Regarding the constructs adopted from PMT, perceived vulnerability and perceived severity, both variables in the threat appraisal process, significantly explain the IT staff's fear arousal concerning the threat of EMR breaches. Furthermore, most variables belonging to the IT staff's coping appraisal process (ie, response efficacy and self-efficacy) also significantly predict the IT staff member's intention to comply with stated privacy policy in addition to response cost. The construct from TRA, namely subjective norm, also significantly predicts the IT staff's intention to comply with a given privacy policy.

The results of this study add to the literature in several ways. First, our study contributes to the literature of EMR privacy policy by integrating PMT and TRA, which may provide a theoretical basis useful in examining privacy policy adherence intentions. Second, our study confirmed that perceived vulnerability and perceived severity may also be regarded as predictors of fear arousal[36] instead of protection motivation.[30,31] Such factor structure may provide a different perspective useful toward an understanding of behaviors related to overall privacy-policy-compliance issues. Third, the findings of this study also provided recommendations for health authorities and hospitals in their planning and design of effective strategies to improve IT staff adherence to privacy policy to ensure the overall safety of EMR.

Appendix A

Questionnaire Items.

Constructs	Items	Source
Perceived vulnerability	I know my hospital could be vulnerable to EMR breaches if I don't adhere to its privacy policy	Ifinedo[38]
	I could fall victim to EMR breaches if I fail to comply with privacy policy	
	I believe that trying to protect hospital's EMR information will reduce illegal access to it	
	My hospital's EMR may be compromised if I don't pay adequate attention to privacy policy	
Perceived severity	I believe the productivity of my hospital and its employees is threatened by privacy-violation incidents	Herath and Rao[39]
	I believe the profitability of my hospitals is threatened by privacy-violation incidents	
Fear arousal	The EMR privacy-violation issue affects my hospital directly	Herath and Rao[39]
	I think EMR privacy-violation is serious and needs attention	
Response efficacy	Every employee can make a difference when it comes to helping to protect the hospital's EMR privacy	Herath and Rao[39]
	Any one individual can do much to help protect the hospital's EMR privacy	
	If I follow the hospital's EMR privacy policy, I can make a difference in helping to protect hospital's EMR	
Self-efficacy	I would feel comfortable following most of the EMR privacy policy my own	Herath and Rao[39]
	If I wanted to, I could easily follow EMR privacy policy on my own	
	I would be able to follow most of the EMR privacy policy even if there was no one around to help me	
Response cost	There are too many overhead costs associated with implementing EMR privacy-protection measures in my hospital	Ifinedo[38]
	Enabling EMR privacy-protection measures in my hospital is/would be time consuming	
Subjective norm	Top management thinks I should follow hospital's EMR privacy policy	Herath and Rao[39]
	My boss thinks that I should follow hospital's EMR privacy policy	
	My colleagues think that I should follow hospital's EMR privacy policy	
	The health information management department in my hospital thinks that I should follow EMR privacy policy	
Behavioral intention to comply	I am likely to follow hospital's privacy policies	Herath and Rao[39]
	It is possible that I will comply with hospital's privacy policy to protect EMR	
	I am certain that I will follow hospital's EMR privacy policy	

Note. EMR = Electronic Medical Records.

Appendix B

Results of f^2 and q^2.

	Fear arousal		Behavioral intention to comply	
	f^2	q^2	f^2	q^2
Perceived vulnerability	0.57	0.35		
Perceived severity	0.06	0.04		
Fear arousal			0.01	0.01
Response efficacy			0.05	0.04
Self-efficacy			0.13	0.10
Response cost			0.00	0.01
Subjective norm			0.26	0.20

Note. $f^2 = (R^2_{included} - R^2_{excluded}) / (1 - R^2_{included})$, $q^2 = (Q^2_{included} - Q^2_{excluded}) / (1 - Q^2_{included})$.

Appendix C

A Comparison of Theoretical Models Used for Organizational Policy Compliance.

Literature	Dependent variable	R^2	Significant predictors	Theory	Sample
Ifinedo[38]	Information systems security policy (ISSP) compliance intention	0.70	Self-efficacy, attitude toward compliance, subjective norms, response efficacy, perceived vulnerability	Theory of planned behavior + PMT	Multiple industries
Vance et al[43]	Intention to comply with security policy	0.44	Perceived severity, rewards, response efficacy, self-efficacy, response cost	PMT + Habit	One municipal organization
Sommestad et al[33]	Intention for IS compliance	0.36-0.45	Perceived norm, perceived behavioral control, Threat appraisal, coping appraisal, anticipated regret	PMT + theory of planned behavior	One defense research organization
Son[59]	Compliance	0.42	Computer self-efficacy, perceived legitimacy, perceived value congruence	Deterrence theory	Multiple industries
Ifinedo[56]	ISSP compliance behavioral intentions	0.61	Attitude toward ISSP compliance, subjective norms, locus of control, self-efficacy	Theory of planned behavior + social cognitive theory social bond theory	Multiple industries
Liang et al[57]	Compliance behavior	0.35	Punishment expectancy, promotion focus × reward expectancy, prevention focus × punishment expectancy	Control theory + regulatory focus theory	Iron and steel industries
Lowry and Moody[58]	Intention to comply with new IS policy	0.57	Existing organizational formal control, new IS policy mandate, reactance to new IS policy	Control theory + reactance theory	Multiple industries

Note. PMT = Protection Motivation Theory; IS = Information Systems.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work has been supported by the Ministry of Science and Technology (Grant MOST-105-2410-H-214-008-MY2), Taiwan, R.O.C.

References

1. Agarwal R, Gao G, DesRoches C, Jha AK. Research commentary—the digital transformation of healthcare: current status and the road ahead. *Inform Syst Res*. 2010;21(4):796-809.

2. Goldschmidt PG. HIT and MIS: implications of health information technology and medical information systems. *Commun ACM*. 2005;48(10):68-74.
3. Zhou L, Soran CS, Jenter CA, et al. The relationship between electronic health record use and quality of care over time. *J Am Med Inform Assoc*. 2009;16(4):457-464.
4. Nguyen L, Bellucci E, Nguyen LT. Electronic health records implementation: an evaluation of information system impact and contingency factors. *Int J Med Inform*. 2014;83(11): 779-796.
5. Abbass I, Helton J, Mhatre S, Sansgiry SS. Impact of electronic health records on nurses' productivity. *Comput Inform Nurs*. 2012;30(5):237-241.
6. Rothstein MA. Health privacy in the electronic age. *J Leg Med*. 2007;28(4):487-501.
7. Kuo KM, Ma CC, Alexander JW. How do patients respond to violation of their information privacy? *HIM J*. 2014;43(2):23-33.
8. Accenture. Getting EMR back in the fast lane. 2014. https://www.accenture.com/us-en/insight-getting-emr-back-fast-lane-summary.aspx. Accessed May 12, 2017.
9. Shu T, Liu H, Goss FR, et al. EHR adoption across China's tertiary hospitals: a cross-sectional observational study. *Int J Med Inform*. 2014;83(2):113-121.
10. Yoshida Y, Imai T, Ohe K. The trends in EMR and CPOE adoption in Japan under the national strategy. *Int J Med Inform*. 2013;82(10):1004-1011.
11. D'Arcy J, Devaraj S. Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sci*. 2012;43(6):1091-1124.
12. Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sci*. 2012;43(4):615-660.
13. Foth M. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *Eur J Inform Syst*. 2016;25(2):91-109.
14. U.S. Department of Health & Human Services. Standards for privacy of individually identifiable health information. 2014. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/introdution.html. Accessed May 12, 2017.
15. R.O.C. Ministry of Justice. Personal Information Protection Act. 2015. http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021. Accessed May 12, 2017.
16. R.O.C. Ministry of Health and Welfare. Regulations governing the utilization and management of electronic medical records among medical facilities. 2009. http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=L0020121. Accessed May 12, 2017.
17. Li T, Slee T. The effects of information privacy concerns on digitizing personal health records. *J Assoc Inf Sci Tech*. 2014;65(8):1541-1554.
18. Martínez S, Sánchez D, Valls A. A semantic framework to protect the privacy of electronic health records with non-numerical attributes. *J Biomed Inform*. 2013;46(2):294-303.
19. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G. Aspects of privacy for electronic health records. *Int J Med Inform*. 2011;80(2):e26-e31.
20. Weber-Jahnke J, Obry C. Protecting privacy during peer-to-peer exchange of medical documents. *Inform Syst Front*. 2012;14(1):87-104.
21. Lafky DB, Horan TA. Personal health records: consumer attitudes toward privacy and security of their personal health information. *Health Inform J*. 2011;17(1):63-71.
22. Samavi R, Consens MP, Chignell M. PHR user privacy concerns and behaviours. *Procedia Comput Sci*. 2014;37:517-524.
23. Vodicka E, Mejilla R, Leveille SG, et al. Online access to doctors' notes: patient concerns about privacy. *J Med Internet Res*. 2013;15(9):e208.
24. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. *J Am Med Inform Assoc*. 2013;20(1):7-15.
25. Greenberg MD, Ridgely MS, Bell DS. Electronic prescribing and HIPAA privacy regulation. *INQUIRY: J Health Car*. 2004;41(4):461-468.
26. Encinosa WE, Bae J. Electronic medical records—federal standards needed. *INQUIRY: J Health Car*. 2006;43(4):307-308.
27. Ma CC, Kuo KM, Alexander JW. A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Med Inform Decis*. 2016;16:13.
28. Eikey EV, Murphy AR, Reddy MC, Xu H. Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings. *Int J Med Inform*. 2015;84(12):1065-1075.
29. Vroom C, von Solms R. Towards information security behavioural compliance. *Comput Secur*. 2004;23(3):191-198.
30. Rogers RW. A protection motivation theory of fear appeals and attitude change. *J Psychol*. 1975;91(1):93-114.
31. Rogers RW. Cognitive and psychological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT, Petty, R eds. *Social Psychophysiology*. 1st ed. New York, NY: Guilford; 1983:153-176.
32. Fishbein M, Ajzen I. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley; 1975.
33. Sommestad T, Karlzén H, Hallberg J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf Comput Secur*. 2015;23(2):200-217.
34. Milne S, Sheeran P, Orbell S. Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *J Appl Soc Psychol*. 2000;30(1):106-143.
35. Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quart*. 2015;39(4):837-864.
36. Tanner JF Jr, Hunt JB, Eppright DR. The protection motivation model: a normative model of fear appeals. *J Marketing*. 1991;55(3):36-45.
37. Floyd DL, Prentice-Dunn S, Rogers RW. A meta-analysis of research on protection motivation theory. *J Appl Soc Psychol*. 2000;30(2):407-429.
38. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput Secur*. 2012;31(1):83-95.
39. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur J Inform Syst*. 2009;18(2):106-125.
40. Arthur D, Quester P. Who's afraid of that ad? applying segmentation to the protection motivation model. *Psychol Market*. 2004;21(9):671-696.

41. Zhang L, McDowell WC. Am I really at risk? determinants of online users' intentions to use strong passwords. *J Internet Commerce*. 2009;8(3-4):180-197.
42. Johnston AC, Warkentin M, Siponen M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quart*. 2015;39(1):113-134.
43. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. *Inform Manag*. 2012;49(3-4):190-198.
44. Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. *MIS Quart*. 2010;34(3):549-566.
45. Churchill GA Jr. A paradigm for developing better measures of marketing constructs. *J Marketing Res*. 1979;16(1):64-73.
46. Jarvis CB, MacKenzie SB, Podsakoff PM. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *J Consum Res*. 2003;30(2):199-218.
47. Boudreau MC, Gefen D, Straub DW. Validation in information systems research: a state-of-the-art assessment. *MIS Quart*. 2001;25(1):1-16.
48. Hair JF, Hult GTM, Ringle CM, Sarstedt M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: Sage; 2014.
49. R Core Team. R: A Language and Environment for Statistical Computing. Vienna, Austria: R Foundation for Statistical Computing; 2013. http://www.R-project.org/. Accessed May 12, 2017.
50. Monecke A, Leisch F. semPLS: structural equation modeling using partial least squares. *J Stat Softw*. 2012;48(3). https://www.jstatsoft.org/index.php/jss/article/view/v048i03/v48i03.pdf. Accessed May 12, 2017.
51. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *J Marketing Res*. 1981;18(1):39-50.
52. Nunnally JC, Bernstein IH. *Psychometric Theory*. 3rd ed. New York, NY: McGraw-Hill; 1994.
53. Hair JF, Black WC, Babin BJ, Anderson RE. *Multivariate Data Analysis: A Global Perspective*. Upper Saddle River, NJ: Prentice-Hall; 2010.
54. Vinzi VE, Trinchera L, Amato S. PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement. In: Vinzi VE, Chin WW, Henseler J, Wang H, eds. *Handbook of Partial Least Squares: Concepts, Methods and Applications*. 1st ed. New York, NY: Springer Science & Business Media; 2010: 47-82.
55. Wetzels M, Odekerken-Schröder G, van Oppen C. Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *MIS Quart*. 2009;33(1):177-195.
56. Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Inform Manag*. 2014;51(1):69-79.
57. Liang H, Xue Y, Wu L. Ensuring employees' IT compliance: carrot or stick? *Inform Syst Res*. 2013;24(2):279-294.
58. Lowry PB, Moody GD. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Inform Syst J*. 2015;25(5):433-463.
59. Son JY. Out of fear or desire? toward a better understanding of employees' motivation to follow IS security policies. *Inform Manag*. 2011;48(7):296-302.