J Med Syst (2017) 41: 198
https://doi.org/10.1007/s10916-017-0833-1

SYSTEMS-LEVEL QUALITY IMPROVEMENT

A Deterrence Approach to Regulate Nurses' Compliance with Electronic Medical Records Privacy Policy

Kuang-Ming Kuo[1] · **Paul C. Talley**[2] · **Ming-Chien Hung**[3] · **Yen-Liang Chen**[1]

Received: 9 August 2017 / Accepted: 3 October 2017 / Published online: 3 November 2017

Abstract Hospitals have become increasingly aware that electronic medical records (EMR) may bring about tangible/intangible benefits to managing institutions, including reduced medical errors, improved quality-of-care, curtailed costs, and allowed access to patient information by healthcare professionals regardless of limitations. However, increased dependence on EMR has led to a corresponding increase in the influence of EMR breaches. Such incursions, which have been significantly facilitated by the introduction of mobile devices for accessing EMR, may induce tangible/intangible damage to both hospitals and concerned individuals. The purpose of this study was to explore factors which may tend to inhibit nurses' intentions to violate privacy policy concerning EMR based upon the deterrence theory perspective. Utilizing survey methodology, 262 responses were analyzed via structural equation modeling. Results revealed that punishment certainty, detection certainty, and subjective norm would most certainly and significantly reduce nurses' intentions to violate established EMR privacy policy. With these findings, recommendations for health administrators in planning and designing effective strategies which may potentially inhibit nurses from violating EMR privacy policy are discussed.

Keywords Deterrence theory · Detection certainty · Electronic medical records · Intention to violate privacy policy · Punishment severity · Punishment certainty · Subjective norm

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Ming-Chien Hung
chemyhmc566@gmail.com

[1] Department of Healthcare Administration, I-Shou University, Kaohsiung City, Taiwan

[2] Department of Applied English, I-Shou University, Kaohsiung City, Taiwan

[3] Department of Information Management, Nanhua University, Chiayi County, Taiwan

Introduction

Hospitals have become critically aware that electronic medical records (EMR) may bring about tangible/intangible benefits, which may include reduced medical errors, improved quality-of-care, curtailed costs, and allowed access to patient information by healthcare professionals without time/space limitations [1, 2]. However, increased institutional dependence on EMR has led to a corresponding increase in the deleterious impact of EMR breaches. These virtual incursions refer to unauthorized access to EMR by internal employees, or outsiders, akin to our study. Such violations may cause tangible/intangible damage to both organizations and individuals [3]. In particular, since the use of accessing EMR on mobile devices has increased almost exponentially, the real probability of EMR breaches has also been on the rise.

Recently, literature has pointed out the importance of employee compliance to organizational policies useful to model overall proper attitude or behavior concerning how organizational resources should be used [4–6]. To protect the inherent privacy of patients' and institutional EMR, coercing hospital employees to comply with EMR privacy policy has become a necessity much in keeping with other organizations [7]. EMR privacy policy refers to a formal statement articulating the privacy rules of a hospital and how it concerns all employees

who have access to EMR and related informational assets [8]. Further, several investigatory attempts have been made regarding how best to deter employees' malicious behavior toward organizational digital assets or how to coerce employees to comply with organizational policy [4, 6, 9–23]. Among the abovementioned studies, several valid attempts have been made to focus specifically on how to motivate healthcare employees to comply with EMR privacy policy or data protection regulations [6, 20–24].

The previous studies may be said to have contributed to an overall understanding of these relative issues. In the named studies, scholars exploring these issues have centered upon a variety of theories in both healthcare and non-healthcare contexts, such as technology acceptance model [23], principal agents theory [13], protection motivation theory [14, 21, 24], health belief model [6], theory of planned behavior [5, 22], decomposed theory of planned behavior [20], theory of reasoned action [21], rational choice theory [19], or deterrence theory, which was most frequently employed [4, 5, 9–13, 15, 18, 19, 22, 25]. Deterrence theory, to the best of our knowledge in reviewing related studies, was however less adopted to investigate healthcare professional's compliance behaviors. One is the study by Foth [22], he used variables taken from the theory of planned behavior and deterrence theory to explain how a hospital staff member's intention to follow data protection regulations may come about. This study surely provided several important and insightful implications for academics and for practical applications. Deterrence theory primarily focuses upon the effect of sanctions useful to deter possible illicit acts [26]. The sanctions imposed are usually divided into formal sanctions (legally binding) and informal sanctions (non-legally binding). But, in his study, Foth [22] incorporated only formal sanctions (i.e., punishment severity and detection certainty). Without informal sanctions to draw some conclusions from, it may be insufficient to locate the correct determinants necessary to compare and then to accumulate subsequent findings. Our study aimed to address this gap in order to better understand the effects of deterrence in a privacy policy compliance context.

However, the effect of deterrence theory constructs on employees' presumed violations or expected compliance with established organizational policy is usually a mixed bag at best. For example, the construct of formal sanctions (e.g., severity of penalty, punishment, and certainty of sanction) was found to provide several significant predictors of information systems security policy compliance in various studies [9, 13], but they were deemed insignificant in yet other studies [18, 19]. On the other hand, the construct of informal sanctions, such as subjective norm, also yielded inconsistent results [14, 17–19, 22]. Further, scarce studies have been conducted on the abovementioned issues as they pertained to diverse healthcare industries, especially whenever they are focused on EMR privacy matters. One of the unique aspects that relates to the healthcare context is that there are greater risks whenever sensitive healthcare information is compromised than there are in other contexts [27]. Hence, it is not only essential, but it is also timely, to explore such issues since EMR is ubiquitous.

Despite it being well known that coercing employee's compliance with privacy policy is institutionally important, there still remains a dearth of information that will aid practice administrators to confront this issue and then focus their efforts accordingly. Broadly speaking, hospital employees who gain access to EMR are potential threats to the patient privacy and institutional integrity, and they should be addressed directly. Nursing staff make up the largest portion of healthcare professionals located in hospitals, and they are the ones who interact most with EMR and patients due to the nature of their work [28]. The intentional or unintentional failure of nursing staff to safeguard patient privacy may erode nurse/patient relationships, jeopardize the quality of the treatment to be provided, and it may even cause serious personal harm to patients [29, 30]. However, scant incidence of study [20] has specifically been focused on nursing staff in hospitals and in the literature. Foth [22] also suggests research must be made to differentiate the effects in hospitals among different occupational groups regarding the protection of patient information against potential breaches. Hence, the primary purpose of this study was to explore those factors that best deter nurses and nurse practitioners from violating EMR privacy policy for any reason by drawing upon the literature of deterrence theory [26, 31].,

Theoretical Foundation, Research Model and Hypotheses

Theoretical Foundation – The Deterrence Theory

Deterrence theory, originating from the criminology discipline, presumes that individuals should make rational decisions toward committing any criminal activity based on a trade-off between inherent benefits and supposed costs [32]. As such, when the benefits are considered to be greater than the costs, individuals may choose to pursue crime [33]. The deterrence theory asserts that individuals' illegal behaviors can be dissuaded via the imposition, with some degree of certainty, of severe and certain legal sanctions [26, 31]. It is supposed that the more severe an act of punishment, the more likelihood that a rational individual will not engage in criminal acts. Further, the certitude of sanctions refers to a punishment that is certain to occur whenever criminal behavior is committed, and the perpetrator is apprehended. More specifically, if a punishment is severe enough and certain enough, individuals will most likely assess the given gains and losses before undertaking in criminal acts. Therefore, it may be assumed that rational individuals will be deterred from illegal conduct if the loss outweighs the gains [34, 35]. Later deterrence studies [13,

14, 17, 36] have further proposed the construct of detection certainty (referring to an individual's perception of the probability of being caught due to the commission of unlawful behaviors) since organizational rules will be considered as useless if these rules are not enforced. Employees will thus seek to comply with the stated organizational rules if they perceive a greater chance of being caught for some non-adherence of those rules.

Further, classic deterrence theory primarily focuses on how the effect of legal sanctions deters illicit acts [26]. Recent studies have noted that informal sanctions such as social disapproval (e.g., subjective norm), self-disapproval (e.g., shame), and moral inhibition can also serve as a deterrent to deviant behaviors [32, 33] or, as a motivator to engage in lawful behaviors [17]. It should be noted that an individual may perceive an unlawful act to be morally offensive [32]. For example, Piquero and Tibbetts [37] incorporated a battery of moral beliefs (i.e., individual judgment of right and wrong about the intended act) and situational shame (i.e., losing self-esteem or a feeling of sin about the intended act) to better understand their putative influence on individuals' intentions to shoplift or to drive while intoxicated. They found both moral beliefs and situational shame significantly reduced respondents' intentions to engage in the above behaviors. Consequently, both formal and informal sanctions may pose threats which individuals will not necessarily take into consideration when deciding on whether or not to participate in unlawful behaviors [33].

Research Model and Hypothesis Formulation

To explore the factors that inhibit nursing professionals from violating stated privacy policy, the researchers used the deterrence theory as a theoretical underpinning. The deterrence theory postulates that formal and informal sanctions can be used as effective deterrents of individuals' illicit acts [32, 33].

Fig. 1 shows the proposed research model, as based upon the deterrence theory. The dependent variable in our study is an intention to violate privacy policy, referring to the subjective probability that a member of the nursing staff will fail to comply with privacy policy in the future. We argue that the imposition of appropriate sanctions based on deterrence theory will diminish nursing staff's illicit intention towards EMR privacy policy. Following the suggestion of Herath and Rao [13], we included three constructs for formal sanctions (i.e., punishment severity, punishment certainty, and detection certainty). As the severity and the certainty of formal sanctions increase, the level of incidence for the illicit act decreases [13]. In our study context, hospitals are obligated to formulate rigorous EMR privacy policies that will regulate employees in order to protect patient privacy and institutional integrity, and when staff violate such policy statements, they will receive severe punishment if culpable for any EMR breaches. Further, Taiwanese hospitals that have adopted EMR policy must assiduously monitor employees' EMR access logs according to proscribed governmental regulation [38]. In words, hospitals must detect suspicious activities to secure the inherent privacy of EMR, and then see to it that violators are sanctioned. This notion is also supported by set standards of information security management, such as the International Standard Organizations (ISO) 17799 (now referred to as the ISO 27002), which suggest that organizations monitor employees' system access and usage to enable enforcement of sanctions and also to achieve certainty / surety of some form of sanctions being imposed [39]. Concerning informal sanctions, we included subjective norm to represent informal sanctions according to the deterrence theory and related studies [32, 33, 36]. Most nurses may perceive it to be morally wrong and morally unacceptable if they do not adhere to established privacy policies since nursing is a highly regulated healthcare industry [40].

Finally, in order to prevent the unexpected influence of some demographic variables to rest on the analysis results, we followed suggested procedures [41] which included demographic variables used as control variables in our proposed model. No hypotheses were required to make up for the control variables [41]. In their study of deterrence across cultures, Hovav and D'Arcy [15] found that age have a significant relationship with IS misuse intention in the U.S. sample. Gender was excluded from as a control variable due to the small male ration (3.82%) found in our sample, which is in line with the fact that most nursing staff are female in Taiwan. Further, educational level and working experiences may be related to nursing staff's knowledge of and familiarity with privacy policies, and it may further influence one's tendency to violate the policies in organizations as well [14, 17]. The justification of the model, along with the research constructs and their associations in the proposed model, was demonstrated as follows.

In this study, punishment severity refers to the nursing staff's perceived degree of punishment [10]. According to

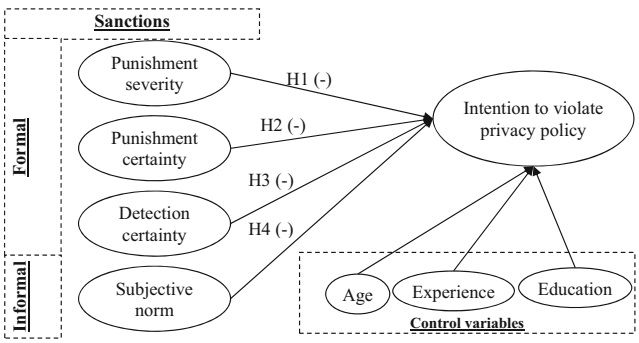


Fig. 1 Research model

the deterrence theory [26], if the level of a punishment increases, a given individual is less likely to undertake unlawful behaviors. In other words, when the nursing staff perceives a stringent degree of punishment for violating privacy policy is possible, they will be less likely to engage in such illegal behavior. Otherwise, there is every likelihood that the nursing staff will be punished by severe civil penalties, criminal penalties, or both if they are caught violating stated privacy policy. Prior studies of information security also lend support to this notion [1, 10, 13, 15, 22, 36].

Punishment severity and punishment certainty have the potential to regulate individuals' behaviors [26, 31]. In this case, punishment certainty means that a nursing staff's perceived probability of being punished is related to noncompliance with stated EMR privacy policy [10]. On the other hand, deterrence theory assumes that potential perpetrators are made aware of prior efforts, including the imposition of rules and punishment to prevent deviant behaviors [13]. Rules for regulating employees, however, will not work if the rules are not enforced with some degree of regularity [42]. According to the theory, if the nursing staff's misbehaviors are caught and they know they will be punished for such misbehavior, the nursing staff will then be more likely not to violate stated privacy policy. Prior studies of information security also support this notion [15, 25, 43].

Detection certainty in this case is considered to be the nursing staff's perception of any probability of being caught if they do not choose to adhere to privacy policy [17]. As discussed in a previous hypothesis, the deterrence theory assumes that potential perpetrators are pre-informed of the punishments meted for unlawful behaviors such as the violation of organizational rules [13]. Enforcing organizational rules and expected punishment is however possible only if organizations are capable of detecting employees' mis-behaviors [13, 42]. Hence, a nursing staff's non-adherence to following privacy policy can be deterred through inspection and auditing their EMR usage patterns of behavior in order to monitor noncompliance [22].

For this study, subjective norm refers to the nursing staff's subjective beliefs regarding their degree of disapproval for nonadherence to EMR privacy policy among those who are important to the nursing staff [17]. The deterrence theory posits that an individual who holds a behavior to be morally offensive will be less likely to commit such reprehensible unlawful behaviors [32, 33]. Similarly, in order to meet the expectations of important others, the nursing staff will be less likely to violate EMR privacy policy on their own, which will be regarded as an act morally offensive by others who are important to the nursing staff. Previous studies have found that an employee's attitude related to IS security policy compliance can be affected by significant others [4, 7, 13, 17, 22, 44].

Based upon the previous discussion, the proposed hypotheses and supportive literature are summarized in Table 1.

Method

Measures

The questionnaire used in this study is comprised of two parts. The first section gathers the respondents' demographic information, and the second part deals with respondents' perceptions concerning the five constructs investigated (punishment severity, punishment certainty, detection certainty, subjective norm, and intention to violate privacy policy). Our study constructs were measured by utilizing previously validated instruments [7, 13, 14, 19, 45, 46], and all items were measured on a seven-point Likert scale (e.g., one for *strongly disagree*, and seven for *strongly agree*). Regarding the detailed sources of items, punishment severity was measured using two items adapted from Herath and Rao [13]. Punishment certainty was measured using two items in accordance with Siponen, Pahnila and Mahmood [45] and Siponen and Vance [19]. Detection certainty was measured using three items adapted from Herath and Rao [13] and Li, Zhang and Sarathy [17]. Subjective norm was measured using three items based on Ifinedo [7]. Intention to violate privacy policy was measured using three items adapted from Chan, Woon and Kankanhalli [46].

The draft questionnaire was then reviewed by experts, including two healthcare information management researchers and two experienced nursing management practitioners. The experts were encouraged to provide feedback about the clarity and validity of the scale that was used. Opinions were compiled as a modification reference for the final version of the questionnaire. Afterwards, a pilot test was conducted to establish the scales via a sampling 20 nursing staff members employed at a single medical center. Slight alterations of words and phrases were made to given items which resulted in a final instrument justified for further validating.

Sampling

We obtained approval from the institutional review board of a large hospital prior to proceeding with the investigation. The subject hospital, a 740-bed Taiwanese hospital employing about 474 registered nurses, was chosen due to the consideration that it is rather active in using EMR in Taiwan in terms of both volume of internal EMR utilization and the amount of EMR exchanged with other hospitals [47]. Prior to the delivery of the questionnaires, we successfully contacted the relevant nursing department to secure their collaboration. We assigned a coordinator for those units of the nursing department that were willing to help with the distribution and collection of the questionnaires per se. Totally, we distributed 300 questionnaires to those units. Subjects were invited to voluntarily and anonymously complete the paper-and-pencil survey. In all, 280 responses were

Table 1 Proposed relationships among key constructs and supportive literature

Hypothesis	Supportive literature
Punishment severity ➔ Intention to violate privacy policy	[1, 11, 13, 15, 22, 36]
Punishment certainty ➔ Intention to violate privacy policy	[15, 25, 43]
Detection certainty ➔ Intention to violate privacy policy	[13, 22]
Subjective norm ➔ Intention to violate privacy policy	[4, 7, 13, 17, 22]

collected, indicating a response rate of 93.33%. Excluding 18 incomplete survey responses due to partial answers, we were left with 262 responses useful for later analysis.

Results

Demographics Analysis

Of the 262 responses, most respondents were female (96.18%). Nearly 96% of the respondents were aged between 20 and 49 years-old. Further, the majority of respondents have a college- or university-level diploma (91.22%). Non-managerial level nurses are the largest group of the respondents (93.51%) and over 66% of respondents have more than 4 years of working experience in the healthcare industry. All respondents are required to use EMR during patient care procedures, indicating the respondents are qualified for participation in our study. Details of the respondents are shown in Table 2.

Data Analysis

Measurement Model Estimates

The proposed model and hypotheses were empirically validated by utilizing partial least square (PLS). We assessed the PLS measurement model by use of three tests: reliability, convergent validity, and discriminant validity [48, 49]. Composite reliability (CR) is used to assess the reliability [48, 49]. The CR of all constructs in our study (*See* Table 3) were higher than the threshold of 0.7 (*See* Table 2) [49]. For convergent validity, the average variance extracted (AVE) of the constructs investigated were larger than the suggested criterion of 0.5 [48]. Moreover, the inter-construct correlations matrix (*See* Table 4) reveals that the square root of AVE for each construct was higher than the correlation of the specific construct with any other constructs in the model [48]. Based on the results, our study demonstrated sufficient reliability and validity for the constructs investigated.

Structural Model

We used a bootstrapping procedure to test the structural model and the significance of each path coefficient. Fig. 2 depicts the structural model results with path coefficient and p values, and Table 5 summarizes the results of hypotheses testing. According the analysis results, we did not find evidence to support hypothesis H1. That is, punishment severity was not significantly associated with the nursing staff's intention of violating EMR privacy policy ($\beta = -0.00$, $p > .05$). Regarding hypothesis H2, the results supported that

Table 2 Descriptive statistics of respondents' characteristics

Profile	Items	Frequency	Percentage (%)
Gender	Male	10	3.82
	Female	252	96.18
Age	20–29	103	39.31
	30–49	150	57.25
	50–64	9	3.44
Education	High school	3	1.15
	College	71	27.10
	University	168	64.12
	Graduate school	20	7.63
Title	Managerial level	17	6.49
	Non-managerial level	245	93.51
Experiences in the healthcare industry (# of years)	1–3	88	33.59
	4–6	39	14.89
	7–9	26	9.92
	> = 10	109	41.60

Table 3 Reliability and validity

Constructs [Source]	Items	Loadings	CR	AVE
Punishment severity [13]	My hospital disciplines employees who break EMR privacy rules	0.90	0.92	0.79
	My hospital terminates employees who repeatedly break EMR privacy rules	0.85		
	If I were caught violating EMR privacy policy, I would be severely punished	0.91		
Punishment certainty [19, 45]	If I don't follow EMR privacy policies, I will be penalized	0.95	0.96	0.92
	I would be formally sanctioned if management learned that I had violated EMR privacy policy	0.96		
Detection certainty [13, 17]	EMR practices are properly monitored for policy violations in my hospital	0.91	0.96	0.89
	If I violate EMR privacy policy, I would probably be caught	0.96		
	If I violate EMR privacy policy, the probability that I would be caught is high	0.95		
Subjective norm [7]	Top management thinks I should follow EMR privacy policy	0.97	0.97	0.94
	My colleagues think that I should follow EMR privacy policy	0.97		
Intention to violate privacy policy [46]	I tend to ignore EMR privacy policy that I think are not necessary	0.95	0.96	0.90
	I tend to ignore EMR privacy policy in order to complete my work quickly	0.96		
	I tend to comply with EMR privacy policy only when it is convenient to do so	0.94		

CR denotes composite reliability; *AVE* denotes average variance extracted

punishment certainty is a significant and negative predictor of the nursing staff's intention to violate privacy policy ($\beta = -0.27$, $p < .001$). Further, we found support of hypothesis H3. That is, detection certainty can significantly reduce the nursing staff's intention of violating privacy policy. Finally, we confirmed that subjective norm negatively contributed to the nursing staff's intention to violate privacy policy ($\beta = -0.41$, $p < .001$), thus supporting hypothesis H4.

Overall, our model explained about 65% of the determined variance in the nursing staff's intention to violate EMR privacy policy. Moreover, the influence of three control variables (i.e., age, experience, and education) revealed that none of the control variables had a significant influence on intention. The results concerning the hypotheses remain unchanged with or without these control variables being present, which means the effects of age, experience, and education are controlled in our model. Further, the global fit index of our study is 0.76 which suggested that our model was in fact valid [50]. Finally, our sample size of 280 is higher than the minimum suggested sample size 166 used to achieve the acceptable 80% statistical power for detecting R^2 values of at least 0.1 (with a 5% probability of error) in terms of our model [49].

Discussion

Key Findings

Protecting the privacy of electronic medical records is an imperative managerial issue given the proliferation and institutional nature of EMR among regular healthcare facility operations. Based upon this understanding, our study aimed to investigate those factors which may prohibit a nursing staff from violating EMR privacy policy based on a foundation of deterrence theory.

The main finding of this study was that both formal and informal sanctions may become effective tools for deterring nursing staff from violating EMR privacy policy. Specifically, formal sanctions including punishment certainty and detection certainty were significantly and negatively related with nursing staff's violating intention while informal sanction including subjective norm can also reduce the nursing staff's intention of violating privacy policy.

Based on the findings, punishment certainty plays an important role in prohibiting the nursing staff from violating privacy policy since they will be less likely involved in violating behaviors if they feel they are found to be responsible for their actions. The results match those observed in earlier studies [15, 42]. Hovav and D'Arcy [15] found that perceived certainty of sanctions can significantly lower an individual's intention to mis-use information systems in the Korean MBA student samples. Second, detection certainty associated negatively with the nursing staff's violating behaviors. The result supports that detection certainty is also an important determinant for preventing nursing staff from violating privacy policy. Increasing the possibility of being caught apparently may lower the nursing staff's perceived ability to violate privacy policy. The significant and negative relationship between detection certainty and intention to violate privacy policy is consistent with prior studies [13, 14, 17] which reported that detection certainty can regulate an individual to compliance with stated organizational policies.

Regarding the construct of subjective norm, there was evidence that informal sanctions such as subjective norm was also effective in deterring the nursing staff from violating privacy policy. This suggests that subjective norm concerning the expectations of important others seem to have an influence on

Table 4 Inter-correlations among constructs

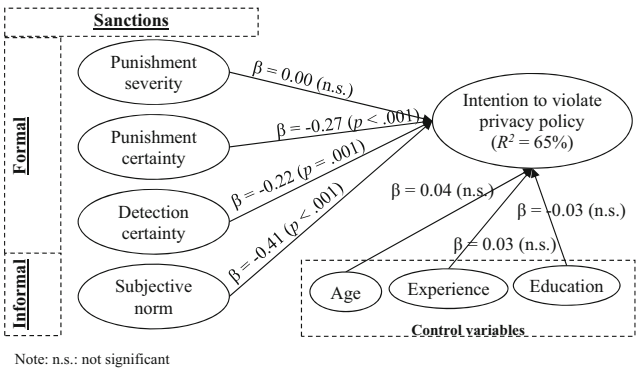
Constructs	A	B	C	D	E
Punishment severity (A)	**0.89**				
Punishment certainty (B)	0.50	**0.96**			
Detection certainty (C)	0.64	0.73	**0.94**		
Subjective norm (D)	0.51	0.66	0.66	**0.97**	
Intention to violate privacy policy (E)	−0.48	−0.70	−0.69	−0.74	**0.95**

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

the behavioral intention of the nursing staff. This finding is in agreement with prior studies [14, 15] which showed social influences such as subjective norm or moral beliefs can deter an individual's mis-behaviors. We, however, didn't find a significant association between punishment severity and nursing staff's intention to violate privacy policy. This result differed from the assertion of the deterrence theory [33]. The deterrence theory, however, has been found to produce paradoxical effects in some prior studies [9, 13, 18, 19]. A plausible reason for the insignificant results in our study may be that rigorous punishments may weaken the nursing staff's trust or loyalty toward hospitals and, thus, exerting a counterproductive influence on their compliance intention of the stated privacy policy.

Significant deterrents of intention to violate privacy policy are likely to include punishment certainty, detection certainty, and subjective norm. They are ranked in order of importance, as follows: subjective norm, punishment certainty, and detection certainty. The results may indicate that informal sanctions (i.e., subjective norm) have a larger effect than formal sanctions (i.e., punishment certainty and detection certainty), which supports Pratt, Cullen, Blevins, Daigle and Madensen [33]'s notion that the threat of non-legal cost sanctions were among the most robust of the deterrence theory predictors. Our findings are also in keeping with previous studies, which found that the effects of informal sanctions are stronger than formal sanctions [12, 13, 15].

Last but not least, with an increasing dependence on mobile devices, the protection of EMR privacy has also become even more complex and multi-dimensional. More and more hospitals are allowing their employees to access EMR via mobile devices such as smartphones, tablets, or laptops in order to perform real-time patient-care tasks inside or outside the hospitals without delay. These mobile devices can even be employees' own devices adding issues related to storage, sharing, and insured confidentiality to the mix. In other words, the concept and application of bringing your own devices (BYOD), referring the practice whereby organizations permit their employees to use their own devices during worktime [51], should not be overlooked when designing and formulating strategies for the protection of EMR privacy.



Note: n.s.: not significant

Fig. 2 Structural model results

Contributions

The results of this study add to the literature in several ways. First, our study contributes to the literature of EMR privacy policy by utilizing the deterrence theory, which provides a feasible theoretical basis, to examine deterrents for privacy policy violation intentions. Specifically, our study empirically validated that both formal and informal sanctions can predict the nursing staff's violating intention. Besides, the findings of this study further provided suggestions for health administrators in their planning and designing of effective strategies necessary for inhibiting the nursing staff from violating policy which is in keeping with the overall expected privacy of EMR.

Academic Implications

For academics, our study helps in the accumulation of knowledge related to the issue of organizational privacy policy adherence/violation. More specifically, this study empirically validated the appropriateness of utilizing the deterrence theory originated from the criminal domain to address how to deter the nursing staff from violating a given privacy policy. By including both formal and informal sanctions, our study found that both kinds of sanctions may be used to deter a nursing staff from violating privacy. Further, the effect of informal sanctions on illicit intention is larger than that of formal sanctions. The result seems to be consistent with Pratt, Cullen, Blevins, Daigle and Madensen [33] assertion that including informal sanctions in a deterrence model will decrease the effect of formal sanctions. Based on the discussions, studies focusing only on formal sanctions may show misleading or inconsistent results.

Table 5 Summary of hypothesis testing results

Hypotheses		Path coefficients	*t*-value	Results
H_1	Punishment severity➔Intention to violate EMR privacy policy	0.00	−0.01	Not supported
H_2	Punishment certainty➔ Intention to violate EMR privacy policy	−0.27***	−4.58	Supported
H_3	Detection certainty➔ Intention to violate EMR privacy policy	−0.22**	−3.44	Supported
H_4	Subjective norm➔ Intention to violate EMR privacy policy	−0.41***	−7.55	Supported

** $p < .05$, *** $p < .001$

Practical Implications

There are also several practical implications that can be derived from our study. First, since punishment certainty was a significant deterrent for the nursing staff's violation of privacy policy, we hold that formal and proscribed sanctions must be required for hospital administrative practices. The primary reason is that these formal sanctions serve as the legal basis for hospitals to take subsequent action against employees who violate stated privacy policy and exist as prior knowledge to exhibit violators' intent. Especially, the design and formulation of these formal sanctions can be considered from the standpoint of different contexts suggested in the literature [51] such as mobile device ownership (how to access EMR), location (where to access EMR), time (when to access EMR), activity (whether as a personal task or patient-care task), and the overall sensitivity of EMR information processed in the era of ubiquitous mobile devices. Second, the support of detection certainty may imply that hospitals should keep good track of the nursing staff's usage of and access to EMR. When they inquire into or update EMR, these actions should be recorded comprehensively for purposes of later auditing. Hence, hospitals should clearly inform their employees that their EMR usage is being monitored anytime and anywhere. Due to the evident characteristics of encrypting or protecting mobile device usage, the detection of EMR intrusion can be a rather challenging task. It is therefore suggested that these monitoring activities should be carefully designed and reviewed in order to ensure that all the EMR access activities are fully logged with whatever devices health professionals have chosen to adopt. Finally, our results further demonstrate that subjective norm deters the nursing staff from violating privacy policy. Hence, managers can improve the nursing staff's compliance intention by enhancing the privacy climate in hospitals and through encouraging colleagues to advocate the negative consequences of violating privacy policy, as the nursing staff's non-compliance intention can be further altered by the opinions of superiors and colleagues. Of course, the negative consequences of violating stated privacy policy, when building the correct privacy-protection climate / domain, cannot be overemphasized. This is especially true since mobile devices are so commonly used to access EMR.

Limitations

Several common limitations may exist in this study. First, the sample is drawn from only one hospital located in Taiwan. Consequently, inferences to the larger population cannot be safely made. In other words, the external validity of the present findings may therefore be confined to a greater or lesser extent due to the adequacy of sample size. Further, the survey conducted in this study was based on self-report rather than observation or the recording of participants' routine behavioral patterns. Future research can thus investigate the issue in order to further understand the relationships among these constructs.

Conclusions

Employees are assumed to be the weakest link in security management [17]. The nursing staff composes the largest portion of healthcare professionals, and they are the ones who interact most with EMRs due to the nature of their work [28]. The chance of EMR being breached will be reduced if the nursing staff are well-regulated to comply with the stated privacy policy of EMR. This is important to hospital administrators because privacy policy compliance means hospitals can better protect the privacy of EMR. By utilizing the deterrence theory, our study proposed and then empirically validated a model in order to explore the deterrent to non-compliance of EMR privacy policy among the nursing staff. The result also demonstrates that our proposed model can explain a sufficient amount of variance (65%) of intention to violate privacy policy. Regarding the constructs for formal sanctions, punishment certainty and detection certainty significantly explains the nursing staff's intention to violate privacy policy. Further, the constructs of informal sanctions, namely

subjective norm, also significantly predict the nursing staff's intention to violate privacy policy.

Funding This work has been supported by the Ministry of Science and Technology (Grant no. MOST-103-2410-H-214-007), Taiwan, R.O.C.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Ethical Approval All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards. This article does not contain any studies with animals performed by any of the authors.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

1. Li, T., and Slee, T., The effects of information privacy concerns on digitizing personal health records. *J. Am. Med. Inform. Assn.* 65: 1541–1554, 2014. https://doi.org/10.1002/asi.23068.
2. Zhou, L., et al., The relationship between electronic health record use and quality of care over time. *J. Am. Med. Inform. Assn.* 16: 457–464, 2009.
3. Culnan, M.J., and Williams, C.C., How ethics can enhance organizational privacy: Lessons from the choicepoint and tjx data breaches. *MIS Quart.* 33:673–687, 2009.
4. D'Arcy, J., and Devaraj, S., Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decis. Sci.* 43:1091–1124, 2012. https://doi.org/10.1111/j.1540-5915.2012.00383.x.
5. Hu, Q., Dinev, T., Hart, P., and Cooke, D., Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decis. Sci.* 43:615–660, 2012. https://doi.org/10.1111/j.1540-5915.2012.00361.x.
6. Sher, M.L., Talley, P.C., Cheng, T.J., and Kuo, K.M., How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Inf. Manag. J.* 46:87–95, 2017. https://doi.org/10.1177/1833358316671264.
7. Ifinedo, P., Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. & Secur.* 31:83–95, 2012. https://doi.org/10.1016/j.cose.2011.10.007.
8. Vroom, C., and von Solms, R., Towards information security behavioural compliance. *Comput. & Secur.* 23:191–198, 2004. https://doi.org/10.1016/j.cose.2004.01.012.
9. Chen, Y., Ramamurthy, K., and Wen, K.W., Organizations' information security policy compliance: Stick or carrot approach? *J. Manage. Inform. Syst.* 29:157–188, 2012.
10. D'Arcy, J., Hovav, A., and Galletta, D., User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inform. Syst. Res.* 20:79–98, 2009.
11. D'Arcy, J., and Hovav, A., Does one size fit all? Examining the differential effects of is security countermeasures. *J. Bus. Ethics*. 89: 59–71, 2009. https://doi.org/10.1007/s10551-008-9909-7.
12. Guo, K.H., and Yuan, Y., The effects of multilevel sanctions on information security violations: A mediating model. *Inform. Manage.* 49:320–326, 2012.
13. Herath, T., and Rao, H.R., Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Supp. Syst.* 47:154–165, 2009.
14. Herath, T., and Rao, H.R., Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* 18:106–125, 2009.
15. Hovav, A., and D'Arcy, J., Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Inform. Manage.* 49:99–110, 2012. https://doi.org/10.1016/j.im.2011.12.005.
16. Hu, Q., Xu, Z., Dinev, T., and Ling, H., Does deterrence work in reducing information security policy abuse by employees? *Comm. ACM*. 54:54–60, 2011.
17. Li, H., Zhang, J., and Sarathy, R., Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis. Supp. Syst.* 48:635–645, 2010. https://doi.org/10.1016/j.dss.2009.12.005.
18. Pahnila, S., Siponen, M., and Mahmood, A., *Employees' behavior towards is security policy compliance (2007) paper presented at 40th annual Hawaii international conference onSystem sciences*. Big Island, Hawaii, pp. 156b–156b, 2007.
19. Siponen, M., and Vance, A., Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quart.* 34:487–502, 2010.
20. Ma, C.C., Kuo, K.M., and Alexander, J.W., A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Med. Inform. Decis. Mak.* 16:13, 2016. https://doi.org/10.1186/s12911-016-0254-y.
21. Sher, M.L., Talley, P.C., Yang, C.W., and Kuo, K.M., Compliance with electronic medical records privacy policy: An empirical investigation of hospital information technology staff. *Inquiry-J. Health. Car.* 54:1–12, 2017. https://doi.org/10.1177/0046958017711759.
22. Foth, M., Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *Eur. J. Inf. Syst.* 25:91–109, 2016. https://doi.org/10.1057/ejis.2015.9.
23. Foth, M., Schusterschitz, C., and Flatscher-Thöni, M., Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in germany. *J Public Health*. 20:253–268, 2012. https://doi.org/10.1007/s10389-011-0456-9.
24. Yang, C.G., and Lee, H.J., A study on the antecedents of healthcare information protection intention. *Inform. Syst. Front.* 18:253–263, 2016. https://doi.org/10.1007/s10796-015-9594-x.
25. Li, H., Sarathy, R., Zhang, J., and Luo, X., Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Inform. Syst. J.* 24:479–502, 2014. https://doi.org/10.1111/isj.12037.
26. Gibbs, J.P., Crime, punishment, and deterrence. *Southwest. Soc. Sci. Q.* 48:515–530, 1968.
27. Anderson, C.L., and Agarwal, R., The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Inform. Syst. Res.* 22:469–490, 2011.
28. Top, M., and Gider, Ö., Nurses' views on electronic medical records (emr) in turkey: An analysis according to use, quality and user satisfaction. *J. Med. Syst.* 36:1979–1988, 2012.
29. Erickson, J. I., and Millar, S., Caring for patients while respecting their privacy: Renewing our commitment. Online J. Issues Nurs. 10, 2005. doi: https://doi.org/10.3912/OJIN.Vol10No02Man01
30. Rindfleisch, T.C., Privacy, information technology, and health care. *Comm. ACM*. 40:92–100, 1997.

31. Tittle, C.R., Crime rates and legal sanctions. *Soc. Probl.* 16:409–423, 1969.
32. D'Arcy, J., and Herath, T., A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *Eur. J. Inf. Syst.* 20:643–658, 2011.
33. Pratt, T.C., Cullen, F.T., Blevins, K.R., Daigle, L.E., and Madensen, T.D., The empirical status of deterrence theory: A meta-analysis. In: Cullen, F.T., Wright, J.P., and Blevins, K.R. (Eds.), *Taking stock: The status of criminological theory*. Transaction Publisher, New Bronswick, NJ, pp. 367–396, 2006.
34. Gopal, R.D., and Sanders, G.L., Preventive and deterrent controls for software piracy. *J. Manage. Inform. Syst.* 13:29–48, 1997.
35. Onwudiwe, I., Odo, J., and Onyeozili, E., Deterrence theory. In: Bosworth, M. (Ed.), *Encyclopedia of prisons & correctional facilities*. Sage Publications, Inc, Thousand Oaks, CA, pp. 234–238, 2005.
36. Siponen, M., Mahmood, M.A., and Pahnila, S., Employees' adherence to information security policies: An exploratory field study. *Inform. Manage.* 51:217–224, 2014. https://doi.org/10.1109/mc.2010.35.
37. Piquero, A., and Tibbetts, S., Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice. Q.* 13:481–510, 1996. https://doi.org/10.1080/07418829600093061.
38. Ministry of Health and Welfare (2009) Regulations governing the production and management of electronic medical records, Retrieved from http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=L0020121 (Accessed 7th July, 2017).
39. Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., The insider threat to information systems and the effectiveness of iso17799. *Comput. & Secur.* 24:472–484, 2005. https://doi.org/10.1016/j.cose.2005.05.002.
40. American Nurses Association (2014) Code of ethics for nurses with interpretive statements, Retrieved from http://nursingworld.org/MainMenuCategories/EthicsStandards/CodeofEthicsforNurses/Code-of-Ethics.pdf (Accessed 10th June 2017).
41. Kock, N., Using warppls in e-collaboration studies: Mediating effects, control and second order variables, and algorithm choices. *Int. J. e-Collab. (IJeC)*. 7:1–13, 2011.
42. Peace, A.G., Galletta, A.G., and Thong, J.Y.L., Software piracy in the workplace: A model and empirical test. *J. Manage. Inform. Syst.* 20:153–177, 2003.
43. Straub, D.W., Effective is security: An empirical study. *Inform. Syst. Res.* 1:255–276, 1990.
44. Ifinedo, P., Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inform. Manage-Amster.* 51:69–79, 2014. https://doi.org/10.1016/j.im.2013.10.001.
45. Siponen, M., Pahnila, S., and Mahmood, M.A., Compliance with information security policies: An empirical investigation. *Comput.* 43:64–71, 2010.
46. Chan, M., Woon, I., and Kankanhalli, A., Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *J. Inform. Priv. Secur.* 1:18–41, 2005.
47. Ministry of Health and Welfare (2017) Bulletin of emrs adoption, Retrieved from http://emr.mohw.gov.tw/emrlist.aspx (Accessed 7th July, 2017).
48. Fornell, C., and Larcker, D.F., Evaluating structural equation models with unobservable variables and measurement error. *J. Marketing Res.* 18:39–50, 1981.
49. Hair, J.F., Hult, G.T.M., Ringle, C.M., and Sarstedt, M., *A primer on partial least squares structural equation modeling (pls-sem)*. Sage, Thousand Oaks, California, 2014.
50. Wetzels, M., Odekerken-Schröder, G., and van Oppen, C., Using pls path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quart.* 33:177–195, 2009.
51. Askar, M.A., and Shen, K.N., Assessment of cybersecurity knowledge and behavior: An anti-phishing scenario, paper presented at the 22nd Americas Concerence on information systems. *San Diego, CA*. 2016:1–10, 2016.