Health Information Management Journal
1–9
© The Author(s) 2016
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1833358316671264
himj.sagepub.com
SAGE

How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments

Ming-Ling Sher, *MPH*[1,2],
Paul C Talley, *PhD*[3],
Tain-Junn Cheng, *MD, PhD*[2,4],
Kuang-Ming Kuo, *PhD*[3]

Abstract

Purpose: The adoption of electronic medical records (EMR) is expected to better improve overall healthcare quality and to offset the financial pressure of excessive administrative burden. However, safeguarding EMR against potentially hostile security breaches from both inside and outside healthcare facilities has created increased patients' privacy concerns from all sides. The aim of our study was to examine the influencing factors of privacy protection for EMR by healthcare professionals. **Method:** We used survey methodology to collect questionnaire responses from staff members in health information management departments among nine Taiwanese hospitals active in EMR utilisation. A total of 209 valid responses were collected in 2014. We used partial least squares for analysing the collected data. **Results:** Perceived benefits, perceived barriers, self-efficacy and cues to action were found to have a significant association with intention to protect EMR privacy, while perceived susceptibility and perceived severity were not. **Conclusion:** Based on the findings obtained, we suggest that hospitals should provide continuous ethics awareness training to relevant staff and design more effective strategies for improving the protection of EMR privacy in their charge. Further practical and research implications are also discussed.

Keywords (MeSH)
electronic health records; health information management; privacy; confidentiality; attitudes; health personnel; Taiwan

Introduction

Electronic medical records (EMRs) are defined as a collection of a patient's medical history that communicate instructions for further medical care and that share laboratory test results by means of software applications (Abbass et al., 2012). Currently, EMRs are widely recognised as a means of improving healthcare quality and reducing financial pressure (Nguyen et al., 2014; Samuel, 2014). EMRs involve the collection of and organisation of medical records electronically, and they serve as the primary storage method for every entailed aspect of patient care (Sykes et al., 2011). As well as avoiding fragmentation and inefficiency of traditional paper-based medical records, EMRs enable healthcare professionals to access patient-related information immediately, regardless of time and location (Zhou et al., 2009). Thus, EMRs are deemed beneficial to the healthcare industry in many aspects. However, on the downside, EMRs are potentially vulnerable to privacy breaches that result in increased concerns among patients (Kuo et al., 2014). Because EMRs have been extensively adopted worldwide (Accenture, 2014; Shu et al., 2014; Yoshida et al., 2013), the real potential for privacy breaches warrants particular and growing concern. In Taiwan, for example, approximately 65.2% of hospitals have adopted EMRs (Ministry of Welfare and Health, 2016), more than 370 hospitals have adopted EMRs and more than 340

[1] National Chung-Cheng University, Taiwan
[2] Chi Mei Medical Center, Taiwan
[3] I-Shou University, Taiwan
[4] Chia-Nan University, Taiwan

Accepted for publication September 01, 2016.

Corresponding author:
Kuang-Ming Kuo, Department of Healthcare Administration, I-Shou University, 8, Yida Road, Yanchao District, Kaohsiung City 82445, Taiwan.
E-mail: kuangmingkuo@gmail.com

hospitals exchange EMRs with one another. In 2012, 44% of healthcare practitioners in the United States had already implemented some form of EMR system in their facilities (Charles et al., 2013). Accenture (2014) predicted that the global EMR market would reach US$22.3 billion by the end of 2015.

Privacy may be defined as 'one's ability to control information about oneself' (Bélanger and Crossler, 2011). Previous studies (e.g. Kuo et al., 2014) have revealed that concerns related to privacy can have a negative impact on patients' perceptions of participating in EMR practices. Moreover, according to a report from the US Department of Health and Human Services (2014), the EMR privacy of nearly 32 million patients has been breached, internally or externally, since 2009. Therefore, it is crucial for hospitals to secure effective privacy measures of EMRs to allay patients' privacy concerns and to ensure compliance with patient institution sharing. Other studies have reported that security breaches continue unabated because employees are themselves the primary cause of breaches (D'Arcy and Devaraj, 2012; Ifinedo, 2014). As a result, hospital employees with both direct and indirect EMR access are all considered to be possible threats to EMR privacy, in addition to any external threats.

The health belief model (HBM) was originally developed to explain preventive health behaviour (Rosenstock, 1974). The HBM posits that the likelihood of an individual to take action in relation to a health condition is fully dependent upon their perceptions of personal susceptibility to and the severity of a health threat. The perceived benefits of a specific health behaviour will be weighed against barriers to the behaviour by those most involved. According to Rosenstock et al. (1994), perceived susceptibility refers to a subjective perception of the risk of contracting an adverse health condition. Perceived severity is the subjective perception regarding to what extent an illness or the consequences of leaving an illness untreated may have a negative impact. Perceived benefit is the subjective perception of how the effectiveness of actions undertaken to reduce threats will lessen the perceived risk. Perceived barrier is the subjective perception of an obstacle that may be encountered while undertaking a recommended behaviour.

Two additional critical variables are included in the notion of HBM: self-efficacy and cues to action (Rosenstock et al., 1994). Self-efficacy is the belief that one can successfully undertake required behaviour to attain expected outcomes and cues to action. For example, receiving advice from others or making one self-aware is a possible trigger that prompts a person to take some sort of preventive action (Rosenstock et al., 1994). The HBM is now widely adopted in various disciplines such as in public health, information systems and transportation (Ng et al., 2009; Şimşekoğlu and Lajunen, 2008; Straub and Leahy, 2014; Wan Omar et al., 2013). Therefore, the model is not only being used to predict individuals' health-related behaviour. On this basis, we argued that the rationale of preventive behaviour derived from the HBM could be transferred to our study in order to consistently predict the privacy protection behaviour of hospital staff, which may also be regarded as a form of inherent preventive behaviour. Furthermore, few studies have attempted to use the HBM to study the privacy protection behaviour of hospital staff in view of the increasing prevalence of EMR adoption among hospital facilities (Accenture, 2014; Shu et al., 2014; Yoshida et al., 2013).

The research question for this study was, 'What are the noticeable factors affecting the EMR privacy-protection behaviour of hospital staff, according to the HBM?' It is generally accepted that all hospital employees having EMR access privileges remain as a possible threat to EMR privacy implementation. Many previous studies have explored the attitudes and perceptions of healthcare professionals towards EMR privacy (e.g. Foth, 2016; Ma et al., 2016). What is lacking is the perspective of other hospital staff. Hence, our study investigated such staff members within the health information management departments, who manage EMRs throughout the hospital setting and also those who are privileged to EMR access capability. By determining the influencing factors, hospitals can effectively develop more and better strategies that will encourage health information management employees to share in protecting EMR privacy. Our study extends the knowledge of the application of HBM in a non-healthcare context, and it also investigates the all-important issue of EMR privacy in a timely fashion. Furthermore, our study may also assist to minimise the gap in the literature due to the missing perspectives from other significant stakeholders, in addition to healthcare professionals, whenever investigating the protection of EMR privacy concerns.

Research framework and hypothesis formulation

Our study used the HBM as the theoretical base upon which to study the volitional intent of health information management staff members to protect EMR privacy. As such, those EMR privacy breaches, which may cause both tangible and intangible damage to both hospital staff and hospitals, refer to unauthorised or unintended access, or both, to EMRs by individuals internal or external to hospitals. According to HBM, an individual will undertake an action relative to a health condition dependent upon the perception of threat to themselves. Transferring this rationale to our study, health information management staff members may react to perceived threats of EMR breaches and thus adopt a coping response that will protect EMR privacy or mitigate against such a threat entirely. Figure 1 shows the six primary factors (i.e. perceived susceptibility, perceived severity, perceived benefit, perceived barrier, self-efficacy and cues to action) said to influence the intention of health information management staff to protect EMR privacy. The justification of the model, along with the research constructs and their associations in the proposed model, was demonstrated as follows.

In our study, perceived susceptibility referred to a health information management staff member's belief of EMR vulnerability to the threat of integrity breaches. The greater a health information management staff member's belief regarding susceptibility to the threat of EMR breaches, he

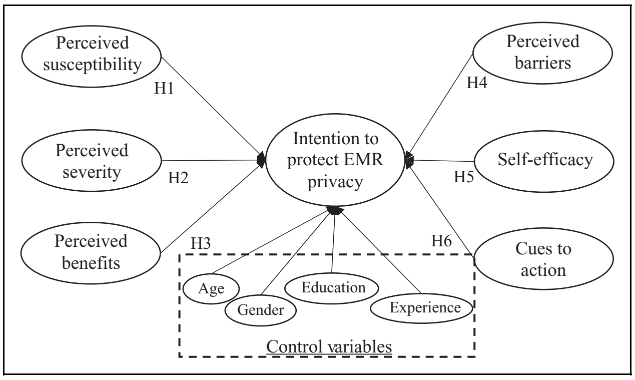

Figure 1. Research framework.

or she will be more active in undertaking the necessary procedures to protect the privacy of EMRs. Several studies (e.g. Ng et al., 2009; Orji et al., 2012) have found that perceived susceptibility is predictive of subsequent preventive behaviour. Thus, the present study hypothesised that:

> **H1:** There is a positive relationship between a health information management staff member's perceived susceptibility and intention to protect EMR privacy.

We defined perceived severity as a health information management staff member's belief concerning the severity of the threat of EMR breaches and the consequences thereof. Akin to perceived susceptibility, the higher a health information management staff member's belief is regarding the severity of negative consequences from EMR breaches, the more vigorous he or she will be to protect the privacy of EMRs. Prior studies (e.g. Kim et al., 2012; Ng et al., 2009) confirmed that perceived severity had an association with health-related behaviour. Thus, the second hypothesis postulates the following:

> **H2:** There is a positive association between a health information management staff member's perceived severity and intention to protect EMR privacy.

Perceived benefit refers to a health information management staff member's belief in the potential benefit of protecting EMR privacy. Therefore, it is only when a health information management staff member perceives the overall benefit of securing EMR privacy that he or she will engage in that protective behaviour. Several studies have reported that perceived benefit is one of the most consistent predictors of health- or preventive-related behaviours (e.g. Kim et al., 2012; Şimşekoğlu and Lajunen, 2008). Based on the discussions, we formulate the following hypothesis:

> **H3:** There is a positive relationship between a health information management staff member's perceived benefit and intention to protect EMR privacy.

Perceived barrier measures the extent to which a health information management staff member's belief regarding the physical and psychological costs to protect EMR privacy. A health information management staff member may hold that despite the effectiveness of protecting EMR privacy to alleviate perceived threat, he or she may still regard the required procedures for such protective behaviour to be inconvenient or costly to him- or herself, which might constrain engagement in such behaviour. Several studies (e.g. Cheney and John, 2013; Kim et al., 2012) have demonstrated that a perceived barrier of costs (e.g. time, money, and effort) can prevent individuals from undertaking health-related behaviours. Based on the discussions, we formulate the following hypothesis:

> **H4:** There is a negative association between a health information management staff member's perceived barrier and their intention to protect EMR privacy.

We measure self-efficacy as the extent of a health information management staff member's belief in his or her ability to effectively protect EMR privacy. A growing body of literature (e.g. Ifinedo, 2014; Ng et al., 2009; Wan Omar et al., 2013) supports the importance of self-efficacy in predicting behavioural intentions. Accordingly, a health information management staff member may tend to protect the privacy of EMR if he or she is confident in undertaking such behaviour. Our study therefore states the following hypothesis:

> **H5:** There is a positive relationship between a health information management staff member's self-efficacy and their intention to protect EMR privacy.

The term 'cues to action' refers to possible behavioural triggers that may cause health information management staff members to protect EMR privacy. Prior literature (e.g. Cheney and John, 2013: 3; Straub and Leahy, 2014) has shown that cues to action can be a predictor of health or preventive behaviour in differing disciplines. Therefore, a health information management staff member may be inclined to protect the privacy of EMRs whenever prompted with reminder messages. Based on the discussions above, the present study hypothesised:

> **H6:** There is a positive association between a health information management staff member's cues to action and their intention to protect EMR privacy.

To diminish unknown influences, we included four control variables in the proposed model: age, gender, experience and education of respondents according to the prior literature (D'Arcy and Devaraj, 2012; Ifinedo, 2014).

Methods

To empirically validate the postulated model, we administered a cross-sectional survey to determine health information management staff members' intention to protect EMR privacy.

Development of measurements

Using Churchill's (1979) recommendations for questionnaire development, we adopted survey items from previously validated studies in order to create an initial pool of

Table 1. Reliability and validity.

Constructs	Items	Mean	SD	λ	AVE	CR	Cronbach's α
Perceived susceptibility	The chance that EMR privacy may be breached is high	3.78	1.23	0.90	0.69	0.94	0.90
	There is a strong probability that EMR privacy breaches may lead to privacy issues	3.95	1.29	0.66			
	The use of EMR is likely to cause privacy problems	3.65	1.18	0.90			
Perceived severity	Having EMR privacy breaches is a severe problem for me	5.47	1.16	0.89	0.80	0.89	0.75
	Losing EMR data is a severe problem for me	5.50	1.19	0.90			
Perceived benefits	Complying with the privacy policy prevents future EMR privacy breaches	5.15	0.99	0.78	0.68	0.90	0.84
	The privacy policy can ensure EMR privacy	4.98	0.95	0.91			
	Complying with the privacy policy prevents the violation of EMR privacy	5.02	1.00	0.92			
	I am less anxious about EMR privacy breaches if I can comply with the privacy policy	4.29	1.22	0.67			
Perceived barriers	Complying with the privacy policy may interfere with many work activities	3.44	1.10	0.71	0.70	0.84	0.61
	Complying with the privacy policy is difficult	3.77	1.22	0.94			
Self-efficacy	I am confident that I can comply with the privacy policy	5.39	0.90	0.86	0.62	0.83	0.69
	I am confident that I can recognise the potential problems of violating EMR privacy	5.11	0.91	0.83			
	I am confident that I can comply with the privacy policy even if there is no one around to help me	4.70	0.97	0.65			
Cues to action	My hospital regularly distributes newsletters or articles concerning the protection of EMR privacy	5.06	0.87	0.84	0.68	0.86	0.76
	My hospital regularly organises talks on EMR privacy	5.13	0.89	0.87			
	My hospital regularly sends out alert messages regarding EMR privacy	5.01	1.02	0.76			
Intention to protect EMR privacy	I intend to protect EMR privacy	5.50	0.82	0.94	0.90	0.96	0.94
	I predict I will protect EMR privacy	5.40	0.88	0.93			
	I plan to protect EMR privacy	5.44	0.85	0.97			

λ: factor loadings; AVE: average variance extracted; CR: composite reliability; SD: standard deviation; EMR: electronic medical records.

survey items for each construct. An expert panel, comprised of two experienced health information management staff members and one scholar who specialised in healthcare information management, inspected proposed items to assess their face and content validity. A few ambiguous words were altered according to the suggestions made by the panel in order to eliminate possible confusion during survey administration. Survey items were measured on a 7-point Likert-type scale, ranging from 1, representing ‘strongly disagree’, to 7, representing ‘strongly agree’. Regarding the detailed sources of items, perceived susceptibility and perceived severity were measured using three and two items, respectively, as adapted from Ng et al. (2009). Perceived benefit and perceived barrier were measured using four and two items, respectively, in accordance with Cheney and John (2013). Self-efficacy and cues to action were both measured using three items adapted from Ng et al. (2009). Intention to protect EMR privacy was measured using three items adapted from Venkatesh and Bala (2008). Since the original items were found in English, it was necessary to first translate these items into Chinese. We used the back-translation (Brislin, 1976) approach to ensure that the meaning of the original items was preserved during the translation between Chinese and English.

Following the suggestion of Straub (1989), recommending that researchers pretest (usually subject to qualitative analysis) and/or pilot test (usually subject to quantitative analysis) instruments before formal investigation, a pretest was then conducted on 10 health information management staff members. Participants were selected by means of convenience sampling in order to establish the scales to be used. Additional modifications to words and phrases were made to the suggested items, resulting in a final scale justified for further testing. Table 1 lists the final survey items.

Ethical approval and sampling method

Ethical approval from the institutional review board of a Taiwanese medical centre was obtained prior to the administration of the survey (IRB#: 10303-L09). In Taiwan, hospitals are categorised into three levels: medical centres, regional hospitals and district hospitals. The total numbers of medical centres, regional hospitals and district hospitals in Taiwan are about 19, 80 and 308, respectively (Joint Commission of Taiwan, 2016). Most of the three hospital levels have adopted EMR due to a huge endeavour made to promote EMR adoption by the Ministry of Health and Welfare in Taiwan. However, medical centres and regional hospitals will usually have more sophisticated EMR systems and wider application of EMR than district hospitals due to available financial resources. Prior to the distribution of the questionnaires, we liaised with nine hospitals, including three medical centres, four regional hospitals and two district hospitals in order to obtain their overall assistance with, and participation in, this study. The nine subject hospitals chosen are considered to be rather active in their utilisation of EMR in Taiwan in terms of their volumes of internal EMR utilisation and also the numbers of EMR exchanged with other hospitals (Ministry of Health and Welfare, 2016). It should be understood that any EMR privacy breaches occurring may have a wider negative impact on the patients; therefore, issues related to privacy protection are especially imperative in these nine hospitals. We appointed a coordinator for each hospital to assist with the distribution and collection of the questionnaires. In total, 291 health information management staff members from the nine hospitals, who have privileged EMR access, were asked to complete the paper-and-pencil survey. Some of these staff members, however, revealed no interest in our survey and did not participate. From 16 April 2014 to 10 June 2014, a total of 240 questionnaires were distributed to the coordinators, of which 230 responses were returned to the researchers. Excluding the 21 incomplete responses due to partial answers, 209 completed responses were used in the final analysis, resulting in a valid response rate of 87.08%.

Results

Characteristics of respondents

Most respondents were female (86.1%), and they were aged from 30 to 39 years (46.9%). Of the respondents, 90.9% were college or university educated. The majority of respondents were located in regional hospitals (56.9%). Most staff members had been working for 10 years or less in health information management departments (67.4%). Detailed characteristics of the respondents and the hospitals are listed in Table 2.

Measurement model evaluation

We first tested the normality of collected data by employing a Kolmogorov–Smirnov test, and the results revealed some extent non-normal distribution ($p < 0.001$). We therefore adopted partial least squares (PLS), which is a method that makes no distribution assumption when analysing the collected data (Hair et al., 2013). Further, the sample size requirement for PLS is ‘ten times the largest number of structural paths directed at a particular latent construct’ (Hair et al., 2013), and our sample size also fits with the requirement. We used R software with a plspm package (R Core Team, 2013; Sanchez, 2013) to inspect both the measurement model and the structural model of PLS, respectively (Hair et al., 2013). The measurement model was used to assess the construct reliability and validity by assessing item loadings, composite reliability (CR), Cronbach’s α, average variance extracted (AVE), discriminant validity and convergent validity (Fornell and Larcker, 1981; Hair et al., 2013). Regarding the measurement model, the item loadings were higher than the 0.6 threshold (Bagozzi and Yi, 1988), indicating sufficient item reliability. The CR of the constructs exceeded the 0.7 threshold (Fornell and Larcker, 1981). Only the Cronbach’s α of the perceived barrier and self-efficacy construct was 0.62 and 0.69, respectively, which were still acceptable (Hair et al., 2010). Furthermore, the AVE of all the constructs was higher than 0.5 (Fornell and Larcker, 1981), demonstrating adequate convergent validity. Finally, discriminant validity was assessed by comparing the square root of AVE with the correlation between two constructs (see Table 3). Our results demonstrated that the square root of AVE was larger than the correlation between the two constructs, indicating adequate discriminant validity.

Table 2. Demographics of respondents.

Variable(s)		Frequency	Percentage
Gender	Male	29	13.9
	Female	180	86.1
Age	20–29	38	18.2
	30–39	98	46.9
	40–49	58	27.8
	≥50	15	7.1
Work experience (years)	≤5	68	32.5
	6–10	65	31.1
	11–15	31	14.8
	16–20	26	12.4
	≥21	19	9.1
Education	High school	19	9.1
	College/university	172	82.3
	Graduate school	18	8.6
Accreditation status of hospitals belonged	Medical centre	75	35.9
	Regional hospital	119	56.9
	District hospital	15	7.2

Structural model evaluation

Regarding the evaluation of the structural model, we also used PLS with bootstrapping to test the structural model and the significance levels of the hypothesised paths. As depicted in Figure 2, perceived benefit ($\beta = 0.12, p < 0.05$), perceived barrier ($\beta = -0.14, p < 0.05$), self-efficacy ($\beta = 0.32$, $p < 0.001$) and cues to action ($\beta = 0.40$, $p < 0.001$) significantly predicted behavioural intention; thus, four (H3 to H6) of the six hypotheses were supported. Perceived susceptibility ($\beta = 0.07, p = 0.223$) and perceived severity ($\beta = 0.07$, $p = 0.219$) were not significant determinants (see Table 4). Overall, approximately 45% of the variance of behavioural intention could be explained by the proposed model. Regarding the three control variables, only gender had a significant effect on intention ($\beta = -0.15, p < 0.05$). However, the results concerning the hypotheses remain unchanged with or without these control variables present.

Furthermore, we adopted the global fit measure (GoF) to evaluate the model fit and it was assessed as: $\sqrt{\overline{\text{Average variance extracted}}\ (\text{AVE}) \times \bar{R}^2}$ (Wetzels et al., 2009). The average AVE = 0.69 and average $R^2 = 0.45$, thus resulting in a GoF = 0.56. As suggested by Wetzels et al. (2009), a GoF value of 0.56 (which exceeds the 0.36 criterion for large effect sizes) indicated that our model was in fact valid.

Table 3. Discriminant validity[a].

	PSU	PSE	PBE	PBA	SE	CTA	ITP
PSU	0.83						
PSE	−0.23	0.89					
PBE	0.00	−0.06	0.82				
PBA	0.41	−0.24	0.06	0.84			
SE	−0.12	0.18	0.29	0.04	0.79		
CTA	0.00	0.22	0.20	0.06	0.40	0.82	
ITP	−0.02	0.23	0.28	−0.07	0.50	0.54	0.95

ITP: intention to protect EMR privacy; CTA: cues to action; PBA: perceived barriers; PBE: perceived benefits; PSE: perceived severity; PSU: perceived susceptibility; SE: self-efficacy.

[a]Diagonal elements are root of the average variance extracted; off-diagonal elements are the correlations among constructs.

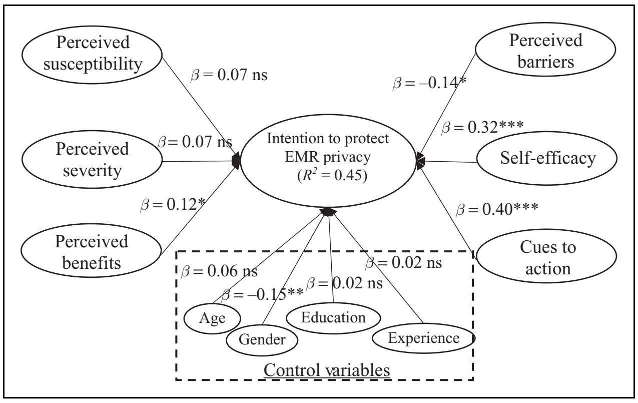

Figure 2. Structural model results. *p < 0.05; **p < 0.01; ***p < 0.001. ns: not significant; β: standardised coefficient.

Table 4. Hypotheses testing results.

Hypotheses	t Statistics	Support?
H1 Perceived susceptibility→Intention to protect EMR privacy	1.22	No
H2 Perceived severity→Intention to protect EMR privacy	1.23	No
H3 Perceived benefits→Intention to protect EMR privacy	2.19[a]	Yes
H4 Perceived barriers→Intention to protect EMR privacy	−2.26[a]	Yes
H5 Self-efficacy→Intention to protect EMR privacy	5.17[b]	Yes
H6 Cues to action→Intention to protect EMR privacy	6.65[b]	Yes

EMR: electronic medical records.

[a]p < 0.05; [b]p < 0.001.

Discussion

Effect of perceived susceptibility on behavioural intention

Surprisingly, the results of the structural model did not support H1. Our results do not corroborate the argument of HBM, which posits that perceived susceptibility significantly predicts subsequent health behaviour. However, Carpenter (2010) found that perceived susceptibility was a weak predictor of preventive behaviour in his meta-analysis of HBM variables. Kim et al. (2012) also reported that perceived susceptibility did not have a significant association with intention to consume healthy food and/or to engage in physical activity by college students. A plausible explanation for the non-significant results in our study may be that the health information management staff members believe that the EMR in their hospitals can be considered as secure because the health authority in Taiwan has regulated hospitals to ensure the security of EMR (Ministry of Health and Welfare, 2009). Hospitals are mandated to afford special attention to the protection of EMR privacy in order to avoid any possible punishment by violating these proscribed regulations (Ministry of Health and Welfare, 2009). Further, no major EMR privacy breaches have been reported since the hospitals involved in this study adopted EMR.

Effect of perceived severity on behavioural intention

In contrast to our expectations, no evidence of significant association between perceived severity and intention was found according to the results; hence, H2 was not supported. Although the results were not parallel with HBM, previous studies have, however, shown that perceived severity exerts a weak effect, or no effect whatsoever, on health behaviour (Janz and Becker, 1984; Kim et al., 2012). In their study of computer security behaviour among employees from differing organisations, Ng et al. (2009) found that perceived severity was not a significant predictor of an employee's computer security behaviour. In light of the mean scores of perceived severity (ranging from 5.47 to 5.50 out of 7) being higher than that of perceived susceptibility (ranging from 3.65 to 3.95), there may be some indication that the respondents were quite concerned about the potential negative consequences of EMR breaches. However, such responses are still insufficient to account for 100% of the variance of their intentions to protect EMR privacy. This is despite their perceived lower scores regarding the possibility of occurring EMR breaches. However, it should be noted that any comparison made will assume that respondents' given approaches to scoring were invariant across perceived susceptibility and perceived severity, which is a point not directly assessed in our current study parameters.

Effect of perceived benefit on behavioural intention

The structural model revealed that the perceived benefit construct is a significant predictor of intention, thus supporting H3. Comparison of the findings is made with those of other studies (Kim et al., 2012; Ng et al., 2009; Şimşekoğlu and Lajunen, 2008) to confirm, as the HBM (Rosenstock et al., 1994) asserts that an individual will engage in a specific behaviour if he or she determines that such behaviour is useful for mitigating a perceived threat. According to the findings, the higher the benefit is of securing the privacy of EMR that health information management staff members can perceive, the more likely they will be to engage in protective behaviour, such as ensuring compliance to privacy policy. Such findings may imply that hospitals should ensure that health information management staff members fully comprehend the effectiveness and content of proscribed EMR privacy policy as well as the importance of compliance to it. Health information management staff members can thus make a proper and appropriate decision to undertake protective behaviour by an adherence to such policy.

Effect of perceived barriers on behavioural intention

The data supported our hypothesis (H4) that a perceived barrier inhibits a health information management staff member's intention to protect EMR privacy. The concept of a perceived barrier was seen to be one of the strongest predictors of health behaviour according to the meta-analysis of Carpenter (2010). Protecting EMR privacy requires compliance with strict regulations, which is typically considered an inconvenience to those most involved; for example, in Taiwan, there are numerous strictly enforced laws requiring the need for hospital staff members to protect the privacy of paper-based medical records. Hence, health information management staff members may already be accustomed to practicing privacy-protection behaviour on a regular basis wherever EMR is involved. Although most of the concepts involved in protecting EMR privacy are the same as those of paper-based medical records, there are still some important differences in protecting EMR. Thus, health information management staff members may perceive more or less difficulty to exact protective behaviour. The findings may also help us to understand that respondents still hold to the notion that rigid privacy protection rules are not so easy to abide by. Hospitals should therefore recheck EMR privacy policy regularly and seek to revise their policy when related regulations or procedures are not practically feasible. Our findings match the study of Kim et al. (2012) on predicting the health behaviour of college students by use of HBM and also with the study of Şimşekoğlu and Lajunen (2008) on predicting seat belt use.

Effect of self-efficacy on behavioural intention

The HBM posits that self-efficacy is a strong determinant of behavioural intention because sufficient skills are required for performing specific behaviour. The finding of our study revealed that self-efficacy is a significant predictor of intention to protect EMR privacy, which mirrors those of previous studies on differing fields (Ifinedo, 2014; Ng et al., 2009; Wan Omar et al., 2013), thus supporting H5. In our study, self-efficacy was the second strongest significant predictor. The significant results may imply that certain skills or concepts (e.g. auditing hospital staff's access log of EMR, exiting EMR system whenever leaving the system unattended or changing passwords periodically) are required for health information management staff members to engage in protecting EMR privacy. Therefore, in addition to providing adequate hardware and software for protecting EMR privacy, hospitals must also equip health information management staff members with the requisite skill set to enhance compliance with the protection of EMR privacy. Possible measures may include regular training on EMR security- and privacy-related issues.

Effect of cues to action on behavioural intention

In our study, the cues-to-action construct was the strongest significant predictor of intention to protect EMR privacy, thus supporting H6. The significant results agree with the findings found in other studies (Orji et al., 2012; Şimşekoğlu and Lajunen, 2008; Straub and Leahy, 2014; Wan Omar et al., 2013). According to these data, we may infer that hospitals should initiate organisational ethics awareness programmes and regularly disseminate privacy protection messages to health information management staff members. Via these awareness programmes, health information management staff members may thus better comprehend and appreciate their roles and responsibilities when dealing with EMR. Further, the system reminder messages should also emphasise the importance of privacy protection and encourage health information management staff members to engage in such protective behaviour whenever, wherever and however possible. With guiding information, health information management staff could be prompted to make discreet decisions on performing appropriate protective behaviour through their own initiative.

Implications and limitations

Practical and research implications. Although the HBM has been proven to be an effective model for explaining intention to protect against a perceived health threat, the literature has primarily focused on human health issues. Our study employed the HBM to predict the behaviour of health information management staff members in their role of protecting EMR privacy. The results revealed that perceived benefit, perceived barrier, self-efficacy and cues to action are significant determinants of health information management staff members' intention to protecting EMR privacy. However, perceived susceptibility and perceived severity were unable to predict intention to protect EMR privacy. Further study could assess the use of the HBM in other contexts to improve an understanding of the possible influences of these constructs.

Regarding practical implications, our results suggest that hospitals should regularly launch ethics awareness programmes to propagate the pertinent knowledge and current practices related to EMR privacy. In particular, hospitals should promote the proven benefits of protecting EMR privacy to encourage health information management staff members to engage in protective behaviour and also to comply with privacy policies that are clear and easy to follow. In addition, hospitals should equip health information management staff members with sufficient hardware and software for protecting EMR privacy, as well as provide them with the required skills to implement protective measures on their own. Finally, hospitals with a vested interest should educate their staff with the latest information and sufficient knowledge on the protection of EMR privacy. In this regard, hospitals may better protect the privacy of EMR and satisfy consumer expectations.

Limitations and future directions. Because our sample comprised only health information management staff members in hospitals, the results should be generalised to other healthcare professionals with caution. Furthermore, we conducted this study in a cross-sectional setting and were unable to determine the changing perceptions of health information management staff over time. Additional insights are required for the postulated model if longitudinal studies are to be undertaken in the future.

Conclusion

On the basis of the HBM, our study validated a research model proposed to improve knowledge of EMR privacy protection among health information management staff members. The results demonstrated that perceived benefit, self-efficacy and cues to action were all significant determinants of intention to protect EMR privacy, while perceived susceptibility and perceived severity were not significant. Although hospital administrators are under increasing pressure to adopt EMR systems to decrease administrative costs and increase access and input efficiency, the issue of privacy cannot be disregarded. The behaviour of hospital staff members plays a crucial role in the protection of EMR privacy; studies exploring the factors that influence staff members' decision to practice vital privacy protection behaviour are thus imperative and requisite for all concerned. To address this knowledge gap, our study scrutinised possible influencing factors using the HBM, with the aim of assisting hospitals to design more effective strategies to improve EMR privacy protection. Moreover, conclusions were also drawn from relevant health theories to explain managerial issues since hospitals increasingly stress the importance and necessity of protecting patients' EMR privacy.

Acknowledgement

We would like to thank Mr Ming-Shan Chang for his help on data collection.

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 article was supported by the Ministry of Science and Technology, Taiwan, ROC (grant no. MOST-104-2410-H-214-007).

References

Abbass I, Helton J, Mhatre S, et al. (2012) Impact of electronic health records on nurses' productivity. *CIN: Computers, Informatics, Nursing* 30(5): 237–241.

Accenture (2014) *Getting EMR back in the fast lane*. Accenture. Available at: http://www.accenture.com/us-en/Pages/insight-getting-emr-back-fast-lane-summary.aspx (accessed 15 April 2015).

Bagozzi RP and Yi Y (1988) On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16(1): 74–94.

Bélanger F and Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly* 35(4): 1017–1041.

Brislin RW (1976) Comparative research methodology: cross-cultural studies. *International Journal of Psychology* 11(3): 215–229.

Carpenter CJ (2010) A meta-analysis of the effectiveness of health belief model variables in predicting behavior. *Health Communication* 25(8): 661–669.

Charles D, King J, Patel V and Furukawa MF (2013) Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008–2012. *ONC Data Brief*, 9. Available at: www.healthit.gov/sites/default/files/oncdatabrief9final.pdf (accessed 7 May 2016).

Cheney MK and John R (2013) Underutilization of influenza vaccine: a test of the health belief model. *SAGE Open* 3(2): 215–239.

Churchill GA Jr. (1979) A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research* 16(1): 64–73.

D'Arcy J and Devaraj S (2012) Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences* 43(6): 1091–1124.

Fornell C and Larcker DF (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(1): 39–50.

Foth M (2016) Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems* 25(2): 91–109.

Hair JF, Black WC, Babin BJ, et al. (2010) *Multivariate Data Analysis – A Global Perspective*. Upper Saddle River: Prentice-Hall.

Hair JF, Hult GTM, Ringle CM, et al. (2013) *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks: Sage.

Ifinedo P (2014) Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. *Information and Management* 51(1): 69–79.

Janz NK and Becker MH (1984) The health belief model: a decade later. *Health Education and Behavior* 11(1): 1–47.

Joint Commission of Taiwan (2016) List of qualified accreditation hospitals and teaching hospitals by the Ministry of Health and Welfare from 2011 to 2015. Available at: www.jct.org.tw/tjcha_CERT/ha.aspx (accessed 7 May 2016).

Kim HS, Ahn J and No JK (2012) Applying the health belief model to college students' health behavior. *Nutrition Research and Practice* 6(6): 551–558.

Kuo KM, Ma CC and Alexander JW (2014) How do patients respond to violation of their information privacy? *Health Information Management Journal* 43(2): 23–33.

Ma CC, Kuo KM and Alexander JW (2016) A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Medical Informatics and Decision Making* 16(1): 13.

Ministry of Health and Welfare (2009) Regulations governing the utilization and management of electronic medical records among medical facilities. Available at: law.moj.gov.tw/LawClass/LawAll.aspx?PCode=L0020121 (accessed 10 May 2016).

Ministry of Health and Welfare (2016) *Bulletin of EMRs Adoption*. Available at: emr.mohw.gov.tw/emrlist.aspx (accessed 10 May 2016).

Ng BY, Kankanhalli A and Xu Y (2009) Studying users' computer security behavior: a health belief perspective. *Decision Support Systems* 46(4): 815–825.

Nguyen L, Bellucci E and Nguyen LT (2014) Electronic health records implementation: an evaluation of information system impact and contingency factors. *International Journal of Medical Informatics* 83(11): 779–796.

Orji R, Vassileva J and Mandryk R (2012) Towards an effective health interventions design: an extension of the health belief model. *Online Journal of Public Health Informatics* 4(3): 4321. Available at: http://ojphi.org/ojs/index.php/ojphi/article/view/4321 (accessed 18 April 2015).

R Core Team (2013) *R: A Language and Environment for Statistical Computing*. Vienna: R Foundation for Statistical Computing, Vienna, Austria. Available at: https://www.R-project.org/.

Rosenstock IM (1974) Historical origins of the health belief model. *Health Education and Behavior* 2(4): 328–335.

Rosenstock IM, Strecher VJ and Becker MH (1994) The health belief model and HIV risk behavior change. In: DiClemente R and Peterson J (eds) *Preventing AIDS*. New York: Springer, pp. 5–24.

Samuel CA (2014) Area-level factors associated with electronic health record adoption and meaningful use in the regional extension center program. *Journal of the American Medical Informatics Association* 21(6): 976–983.

Sanchez G (2013) *PLS Path Modeling with R*. Available at: www.gastonsanchez.com/PLS_Path_Modeling_with_R.pdf (accessed 15 May 2016).

Shu T, Liu H, Goss FR, et al. (2014) EHR adoption across China's tertiary hospitals: a cross-sectional observational study. *International Journal of Medical Informatics* 83(2): 113–121.

Şimşekoğlu Ö and Lajunen T (2008) Social psychology of seat belt use: a comparison of theory of planned behavior and health belief model. *Transportation Research Part F: Traffic Psychology and Behaviour* 11(3): 181–191.

Straub DW (1989) Validating instruments in MIS research. *MIS Quarterly* 13(2): 147–169.

Straub CL and Leahy JE (2014) Application of a modified health belief model to the pro-environmental behavior of private well water testing. *JAWRA Journal of the American Water Resources Association* 50(6): 1516–1526.

Sykes TA, Venkatesh V and Rai A (2011) Explaining physicians' use of EMR systems and performance in the shakedown phase. *Journal of the American Medical Informatics Association* 18(2): 125–130.

US Department of Health and Human Services (2014) *Breaches Affecting 500 or more Individuals*. Available at: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (accessed 16 December 2015).

Venkatesh V and Bala H (2008) Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences* 39(2): 273–315.

Wan Omar WR, Patterson I and Pegg S (2013) Using a health belief model to investigate the walking behaviour of residents living in Kuala Lumpur, Malaysia. *Annals of Leisure Research* 16(1): 16–38.

Wetzels M, Odekerken-Schröder G and van Oppen C (2009) Using PLS path modeling for assessing hierarchical construct models: guidelines and empirical illustration. *MIS Quarterly* 33(1): 177–195.

Yoshida Y, Imai T and Ohe K (2013) The trends in EMR and CPOE adoption in Japan under the national strategy. *International Journal of Medical Informatics* 82(10): 1004–1011.

Zhou L, Soran CS, Jenter CA, et al. (2009) The relationship between electronic health record use and quality of care over time. *Journal of the American Medical Informatics Association* 16(4): 457–464.