Inf Syst Front (2016) 18:253–263
DOI 10.1007/s10796-015-9594-x

A study on the antecedents of healthcare information protection intention

Chang-Gyu Yang[1] · Hee-Jun Lee[2]

Published online: 14 September 2015

Abstract This study investigates the antecedents of HIPI (Healthcare Information Protection Intention) of HIS (Healthcare Information Systems) users by introducing a model which incorporates constructs from GDT (General Deterrence Theory) and PMT (Protection Motivation Theory). The results show that (1) a clear awareness of the consequences of security threats increases HIS users' understanding on the severity of healthcare information leakage, and thus may decreases abuse of HIS by users; (2) user satisfaction with the security system may make them have self-efficacy that they can handle the medical information leakage issue by themselves; and (3) although HIS users are realizing the consequences of healthcare information leakage, they think that they are unlikely to encounter such situations. The results imply that in order to increase HIPI of HIS users, ongoing security education is needed and motivating users to protect healthcare information through their satisfaction with the security system is important.

Keywords Healthcare information system · General deterrence theory · Protection motivation theory · Induction control intention · Self-defense intention · Protection intention

1 Introduction

In terms of cost savings opportunities for healthcare providers and the ability to provide various healthcare services, the convergence of healthcare services and ICT (Information and Communication Technology) is accelerating (Caro 2008; Agarwal et al. 2010; Poba-Nzaou et al. 2014). This paradigm integrally manages various types of patient records in order to facilitate not only cost savings, but also stability of treatment, reduction in wait times, access to the medical team's patient records, by lining PACS (Picture Archiving Communications System), OCS (Order Communication System), etc. to EMR (Electronic Medical Record System) which manages computerized medical records of individuals (Law et al. 1995; Lorence and Spink 2004; Williams and Boren 2008; Chang et al. 2009; Lluch 2011; Teoh et al. 2012). Recently, along with the integration of HIS, it becomes possible to use patient records anytime, anywhere through mobile devices (Hurson et al. 2004; Bønes et al. 2007; Wu et al. 2011; GE 2012; Siemens 2012. That is, we can say that in comparison to the past, the recent HIS environment enables users to read information of all kinds of HIS through various devices by one single certification.

Although the positive aspect of the adoption of HIS include the acceleration of HIS adoption and increase in investment, negative aspects, such as leaking large amount of healthcare information, are occurring due to the computerization of various types of healthcare information (Anderson and Agarwal 2011; He et al. 2012). Even considering only the cases of healthcare information leaked in the United States, patient records have been exposed continuously since the adoption of HIS, and recently the CIO of Utah was resigned due to the data security incident that information of 280 thousand patients

✉ Chang-Gyu Yang
cozlove@ajou.ac.kr

[1] Gyeonggi Tourism Organization, 5Fl., 1150, Gyeongsu-daero, Jangan-gu, Suwon-si, Gyeonggi-do 16207, South Korea

[2] Hana Academy Seoul, Eunpyeong-gu, South Korea

was leaked (GOVTECH 2012). Moreover, 559 cases of personal information leakage were reported a year on average during the period 2008 ~ 2011, and over 20 % of the cases in 2011 were in the field of HIS (ITRC 2012). In particular, since the use of HIS on mobile devises has increased recently, healthcare information leakage is increasing continuously due to users' low security awareness (HIMSS 2012; Mouttham et al. 2012).

Healthcare information is the essential information associating with patients' medical records, which includes sensitive information such as patients' health, names of disease, conditions of disease, courses of treatment, etc. Because the disclosure of such healthcare information may lead to secondary psychological damage to patients who are experiencing physical pain, and the leaked information is possible to be used to commit various crimes that cause serious damage to the society, thorough security is required. However, meanwhile the main stream of research on security of HIS is about the technological aspect (Dhillon and Backhouse 2000; Janczewski and Xinli Shi 2002; Gritzalis and Lambrinoudakis 2004). That is, because previous studies paid attention only to security policies and security systems even though healthcare information leakage is mainly caused by abuse and neglecting management by HIS users, they have limitations in determining the cause of healthcare information leakage, which is due to HIS users who should follow security policies and use security systems.

Therefore, this study mainly focuses on HIPI of users who use HIS in an environment for actual healthcare information protection. This study intends to examine the antecedents of HIPS of users on HIS in an integrated environment where most kinds of HIS can be used not only on PC, but also on mobiles devices through SSO (Single Sign On). In other words, this study aims to identify the influences of deterrence factors on actual HIS users in order to control healthcare information leakage, as well as whether HIPI of these users have been formed. For this purpose, an integrated model incorporating constructs from GDT and PMT are introduced in order to identify the antecedents of HIS users' HIPI, which is the main cause of healthcare information leakage. In particular, because strategies for improvement in security policies and security systems in HIS vary significantly according to the antecedents of HIPI, the study would be helpful to policy makers of healthcare information protection, providers of security systems, and HIS users.

2 Literature review

2.1 Healthcare information systems (HIS)

The need for new HIS is increasing and the changes of social awareness on the field of healthcare information are more diverse in the ubiquitous computing environment along with the development of information technology. General IS (Information System) refers to the aggregation of data, software, and hardware that enables information collection, processing, storage and retrieval for decision making and business management in organizations (Duan et al. 2011). From such a perspective, HIS can be defined as an IS that covers treatments, medical assistances, diagnostic imaging, and all tasks starting from healthcare reception until receiving payments, which supports various decision making, improvement in the quality of healthcare services, and efficient healthcare management associated with treatments in medical institutions. Especially, as a variety of information technologies (Biomedical Signal Processing, wired and wireless communications, IoT, etc.) have been adopted due to the recent growth of U-healthcare, patients' health conditions can be accessed anytime, anywhere (Yao et al. 2012; Siddiqui et al. 2014). Therefore, HIS is an aggregation of various information systems, operating for the purpose of patients' treatments in medcal institutions, as shown in Table 1.

2.2 General deterrence theory (GDT)

GDT is designed to inform individuals of the punishments due to resistance or deviation in order to put them off resisting or deviating (Hupert et al. 1996). In the meantime many studies used the constructs of GDT to explain the intention of information system abuse (Straub and Nance 1990; Harrington 1996; Gopal and Sanders 1997; Kankanhalli et al. 2003; Lee et al. 2004). As shown in Table 2 below, the major constructs can be classified mainly into three categories of constructs. The first construct is the security policy that defines the roles and responsibilities of specific policies for preventing IS abuse (Kwok and Longley 1999; Straub and Nance 1990). Such security policies must have certainty and severity of punishment in order to have an effective deterrent (Straub and Welke 1998; Theoharidou et al. 2005; Herath and Rao 2009). However, even a security policy has certainty and severity, the deterrent effect will be insignificant if users are not aware of the consequences of security threats. Thus, security awareness, the second construct that make users clearly understand the consequences of security threats, is important (Siponen 2000; D'Arcy and Hovav 2009). Finally, together with security policy and security awareness, a security system such as the security of data center that includes supporting software and cable security is also a leading construct (Kwok and Longley 1999; Lee et al. 2004).

2.3 Protection motivation theory (PMT)

As we can see in existing studies that have utilized GDT, recent studies are utilizing constructs which identify individual's protection motivation under GDT and information

Table 1 Major HIS

Classification	HIS	Main function
Medical information support	OCS(Order Communication System)	The most fundamental system in HIS, which is a prescription delivery system transmitting patients' prescriptions between the treatment, treatment support, and hospital administrative departments.
	PACS(Picture Archiving & Communication System)	A picture archiving communication system which transmits medical images regarding the diagnoses of patients after receiving them in a digital form.
	EMR(Electronic Medical)	An electronic medical record which contains all the information regarding patients' clinical practices.
	LIS(Laboratory Information System)	A software system that records, manages, and stores data for clinical laboratories.
Hospital administrative support	PM/PA(Patient Management/Patient Account)	Management on patients' registration and reception/Management on receipts of patients' medical costs.
	EDI(Electronic Data Interchange)	Insurance claims and outpatient prescription
U-Healthcare support	NHS(Network Health System)	A wired and wireless communications-based network platform which is able to transmit biometric information.
	MDHS(Medical Device Healthcare System)	A system which processes, analyzes, stores, and utilizes biometric information.
	SHS(Sensor Healthcare System)	A system which measures and acquires bio-signal by using sensor.

protection intention (Lee et al. 2004; D'Arcy and Hovav 2009; D'Arcy et al. 2009). However, previous studies have the limitation that they used fragmentary variables which cannot comprehensively explain individual protection intention. This study uses Rogers (1983)'s PMT on account of this limitation. Based on the Expectancy- Value Theory (Edwards 1954), Rogers (1983) established PMT, which is widely used in the field of sociology (Rippetoe and Rogers 1987; Milne et al. 2006). PMT is one of the suitable theories to predict individual's protection behaviors, and it stems from the threat appraisal and the coping appraisal (Anderson and Agarwal 2011). If the individual feels the risk, threat appraisal assesses the severity of the consequences of the risky situation, as well the vulnerability as the individual is exposed to the risk (Rogers 1983; Woon et al. 2005). Along with the threat appraisal, the coping appraisal consists of self-efficacy (the belief in one's ability to solve the risk) and response-efficacy (the expectancy that the risk can be avoided in reality) (Woon et al. 2005). In addition, recent studies on information protection intention have put their efforts on identifying prior causes of protection intention (Vance et al. 2012). Therefore, utilizing PMT constructs as mediators of GDT's influence on information protection intention helps identify the formation of individual information protection intention more concretely (Table 3).

Table 2 Major constructs of GDT

Researchers	Security policy	Security awareness	Security system	Mediator variable	Dependent variable
Straub and Nance (1990)	–	DC, DS	RE	–	CA
Kankanhalli et al. (2003)	–	DE, DS	PE	–	ISSE
Lee et al. (2004)	SP	SA	SS	SDI	AI
D'Arcy and Hovav (2009)	SP	SETA	CM	CSEVS	ISMI
D'Arcy et al. (2009)	SP	SETA	CM	PCS, PSS	ISMI
Herath and Rao (2009)	–	SPA, CD NBPB	–	–	PCI
Al-Omari et al. (2012)	SP	SETA	ISE, CM	PUP, PEU	IC

AI = Abuse by Invaders; CA = Computer Abuse; CD = Certainty of Detection; CM = Computer Monitoring; CSEVS = Computer Self-Efficacy Virtual Status; DC = Deterrent Certainty; DE = Deterrent Efforts; DS = Deterrent Severity; IC = Intention to Comply; ISE = Information Security; ISMI = Information System Misuse Intention; ISSE = Information System Security Effectiveness; NBPB = Normative Beliefs Peer Behavior; PCI = Policy Compliance Intention; PCS = Perceived Certainty of Sanctions; PE = Preventive Efforts; PEU = Perceived Ease of Use; PSS = Perceived Severity of Sanctions; PUP = Perceived Usefulness of Protection; RE = Rival Explanations; SA = Security Awareness; SDI = Self Defense Intention; SETA = Security Education, Training, and Awareness; SP = Security Policy; SPA = Severity of Penalty; SS = Security System

Table 3 Major constructs of PMT

Researchers	Antecedent variable	Threat appraisal	Coping appraisal	Dependent variable
Workman et al. (2008)	–	PV, PS	LC, SE, PRE, RCB	OB
Ng et al. (2009)		PSU, PS, PB, PBA	CA, GSO, SE	CSB
Crossler (2010)	–	PV, PS	SSE, RE, PC	BD
Johnston and Warkentin (2010)	–	PTS, PTSU	RE, SE	BI
Anderson and Agarwal (2011)	–	CR, ST	PCE, SB, SE	IPSRB
Ifinedo (2011)	–	PV, PS	RE, RCO, SE	ISSPCBI
Vance et al. (2012)	H	PV, PS, R	RE, SE, RCO	ICISSP

BD = Backup Data; BI = Behavioral Intention; CA = Cues to Action; CR = Concern Regarding; CSB = Computer Security Behavior; GSO = General Security Orientation; H = Habit; ICISSP = Intention to Comply with IS Security Policy; IPSRB = Intentions to Perform Security-Related Behavior; ISSPCBI = ISSP Compliance Behavioral Intention; LC = Locus of Control; OB = Omissive Behavior; PB = Perceived Benefits; PBA = Perceived Barriers; PC = Prevention Cost; PCE = Perceived Citizen Effectiveness; PRE = Perceived Response Efficacy; PS = Perceived severity; PSU = Perceived Susceptibility; PTS = Perceived Threat Severity; PTSU = Perceived Threat Susceptibility; PV = Perceived vulnerability; R = Rewards; RCB = Response Cost-Benefit; RCO = Response Cost; RE = Response Efficacy; SB = Security Behavior; SE = Self-Efficacy; SSE = Security Self-Efficacy; ST = Security Threats

3 Research hypotheses

3.1 GDT and PMT

If HIS users are not clearly aware of the security policy and the consequences of security threats, they will not realize the severity of the consequences of the risky situation and the vulnerability that they are exposed to the risk. In other words, if HIS users are clearly aware of the security policy and the consequences of security threats, they are going to be more aware of the severity and vulnerability due to security threats. Therefore, we state the following hypotheses.

H1a: Security awareness has a positive (+) impact on severity.
H1b: Security awareness has a positive (+) impact on vulnerability.

Furthermore, awareness of security threats is believed to have an influence on HIS users' belief in security policy or their self-confidence to stop the security threats by themselves. That is to say, if HIS users are clearly aware of the consequences of security threats, they are going to pay attention to the effects of the current security policy, and thus they will believe that the security policy can prevent security threats in reality and be confident that they are possible to handle the security threats by their own efforts. Therefore, we suggest the following hypotheses.

H1c: Security awareness has a positive (+) impact on response-efficacy.
H1d: Security awareness has a positive (+) impact on self-efficacy.

Due to the computerization of patients' medical records, the problems of hacking and abuse have been brought up continuously (GOVTECH 2012; ITRC 2012). In response to this issue, European companies like GE and Siemens have released security systems for healthcare information protection (GE 2012; Siemens 2012). In the context of HIS, security system supports a variety of functions from integrated authorization and authority management to encryption of sensitive healthcare information and healthcare system database (Colling and York 2010). The adoption of security systems that provide various functions enables HIS users to have response-efficacy (the belief that adopting security systems will be effective in preventing problems and penalties caused by disclosure and abuse of healthcare information) and self-efficacy (the belief that they can protect healthcare information by themselves through the security systems). Therefore, we propose the following hypotheses.

H2a: Security system satisfaction has a positive (+) impact on response-efficacy.
H2b: Security system satisfaction has a positive (+) impact on self-efficacy.

3.2 PMT and ICI

If HIS users are more aware of the risks of security threats, they will be more aware of that they may be at direct or indirect risks when security incidents happen. That is, if HIS users perceive higher level of severity of the security threats, they will perceive higher level of vulnerability to the security threats. Therefore, we make the following hypothesis.

H3a: Severity has a positive (+) impact on vulnerability.

While using HIS, users consider the severity of the consequences of security threats and the vulnerability that they are always exposed to the security threats (Rogers 1983; Woon et al. 2005). This corresponds to the threat appraisal in PMT. In other words, HIS users have an attitude towards not using HIS illegally while conducting threat appraisal, leading to the decrease in ICI. Moreover, in the context of deterrence system, since users understand and trust the security system a lot, ICI will decrease in case that they believe the actual security policy can prevent the security threats. Therefore, we suggest the following hypotheses.

H3b: Severity has a negative (−) impact on ICI.
H3c: Vulnerability has a negative (−) impact on ICI.
H3d: Response-efficacy has a negative (−) impact on ICI.

3.3 PMT and SDI

While using HIS, users perceive self-efficacy that they have experiences with security functions and are able to protect healthcare information by themselves, and thus can avoid a certain part of punishments when healthcare information leakage occurs (Woon et al. 2005). This corresponds to the coping appraisal in PMT. If HIS users perceived higher level of self-efficacy, they will perceive higher level of response-efficacy, which is their belief in the actual security policy of healthcare information. That is to say, the self-confidence of users that they can solve various security threats by their own ability increases the level of trust that actual security threats are possible to be handled. Therefore, we propose the following hypothesis.

H4a: Self-efficacy has a positive (+) impact on response-efficacy.

Finally, if HIS users realize that the HIS they are using may be exposed to security threats, and they believe in the effect of security policy, they are expected to put extra efforts on healthcare information protection. Besides, in case the users are confident that they can stop the security threats by their own abilities, they will have higher intention to prevent illegal use of HIS. In other words, vulnerability, response-efficacy, and self-efficacy of HIS users are believed to have positive influences on SDI (HIS users' intention to install security program and prevent illegal use by themselves). Therefore, we make the following hypotheses.

H4b: Vulnerability has a positive (+) impact on SDI.
H4c: Response-efficacy has a positive (+) impact on SDI.
H4d: Self-efficacy has a positive (+) impact on SDI.

4 Method and results (Fig. 1)

4.1 Data collection

Survey was conducted among HIS users who work at university hospital in South Korea in order to verify our research model. In terms of scale, this hospital is one of the top ten hospitals in South Korea and it puts a lot of efforts on healthcare information protection, such that it performed DB encryption to strengthen the security system of HIS, install anti-virus programs on PC or use certification to make protection policy compulsory, and so on. Moreover, because an integration of all kinds of HIS is established standing on the basis on EMR that provides OCS/PACS functions, and usage through internet and mobile devices is possible, we considered it as an appropriated target for the survey.

Among the collected questionnaires, excluding 4 questionnaires that contained missing responses or false responses, a total of 222 questionnaires were used in this study. SPSS 15.0 and AMOS 7.0 were the statistical software used for the empirical analysis, and frequency analysis was conducted to analyze the demographic characteristics and general characteristics of the sample. With regard to the demographic characteristics of the survey respondents, the sample consists of slightly more females (124, 55.8 %) than males (98, 44.1 %). Most respondents are in their 30s (90, 40.5 %) in terms of age, and most respondents are university graduates (173, 77.9 %) in terms of education. Regarding occupations of the respondents, the sample consist of 28 (12 %) doctors, 78 (35 %) nurses, and 116 (52 %) medical administrators, showing that all respondents deal with HIS daily. This study provides the operational definitions of factors that have an influence on HIPI based on previous studies, and modified the measurement items in previous research to construct research questions. Table 4 presents the conceptual definitions and antecedents of the research variables.

4.2 Factor analysis

Factor analysis was conducted using SPSS 15.0 to verify the reliability and validity of each construct. The results of exploratory factor analysis are shown in Table 5. The value of Cronbach's α of each element is higher than 0.7, and all the elements have been classified correctly.

Factor analysis was conducted to verify the reliability and validity of each construct. Based on the results, the fit indices $\chi2$ (181, N = 222) = 344.017, p < 0.000, GFI = 0.878, AGFI = 0.830, NFI = 0.927, CFI = 0.964, TLI = 0.954, RMSE = 0.064 indicate stable results and relatively high values. Thus the overall goodness-of-fit is satisfied. Afterwards, in order to

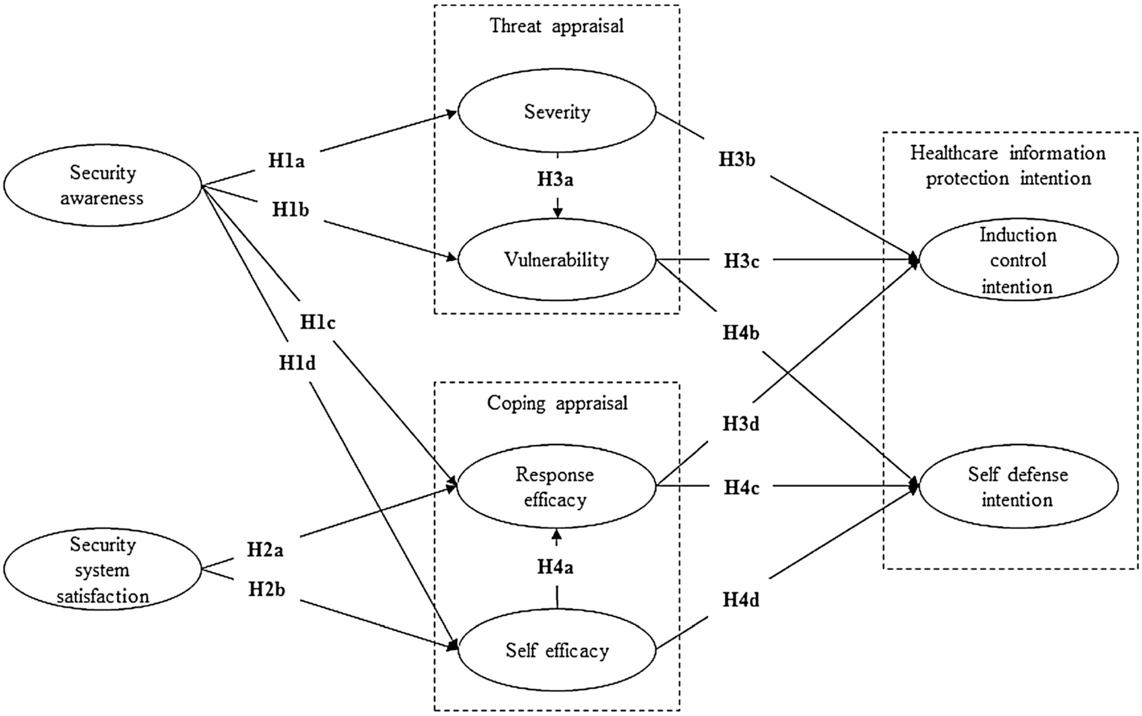

Fig. 1 Research model

evaluate the convergent validity of the measurement items of each construct, standardized factor loadings and standardized residual covariances were verified. As shown in Table 6, the results demonstrate that the reliability and validity of the measurement items that compose each construct exceed the standardized values.

Based on the results of confirmatory factor analysis, the reliability and validity of the measurement items that compose each factor are compatible with the standards. In addition, discriminant validity was assessed by comparing the correlation coefficient and the average variance extracted (AVE) of each construct. According to the results of the correlation analysis between constructs, which are shown in Table 7, we can know that discriminant validity exists according to the diagonal matrix AVE.

Table 4 Conceptual definition of research variables

Research variable	Conceptual definition	References
Security awareness (SA)	The extent of recognition of users who use healthcare information on the security policy and the consequences of security threats	Ajzen (1991), Chan et al. (2005), Herath and Rao (2009), Bulgurcu et al. (2010)
Security system satisfaction (SS)	The extent of users' satisfaction with security system and that they think sufficient investments have been made	Ajzen (1991), Lee et al. (2004)
Severity (SV)	The extent of recognition of the seriousness of security threats while using HIS	Rippetoe and Rogers (1987), Milne et al. (2006), Workman et al. (2008)
Vulnerability (VU)	The extent of recognition on the weakness of health information being exposed to security threats while using HIS	Rippetoe and Rogers (1987), Milne et al. (2006), Workman et al. (2008)
Response-efficacy (RE)	The extent of users' trust in the effect of security policy while using HIS	Rippetoe and Rogers (1987), Milne et al. (2006), Workman et al. (2008)
Self-efficacy (SE)	The extent of users' self-confidence that they can cope with security threats by their own abilities while using HIS	Compeau and Higgins (1995), Workman et al. (2008)
Induction control intention (ICI)	The extent of intention to steal someone else's ID or illegally use HIS without authority	Ajzen (1991), Lee et al. (2004)
Self defense intention (SDI)	The extent of intention of users to install security programs by themselves in order to prevent illegal use of HIS	Ajzen (1991), Lee et al. (2004)

Table 5 Results of exploratory factor analysis

Factor (Cronbach's α)	Elements							
	1	2	3	4	5	6	7	8
SA	**0.824**	0.177	0.257	0.174	0.140	0.153	0.015	0.177
(0.921)	**0.822**	0.170	0.218	0.160	0.183	0.202	-0.059	0.177
	0.809	0.183	0.126	0.047	0.137	0.321	-0.030	0.161
SS	0.164	**0.864**	0.159	0.083	0.228	0.169	−0.042	0.062
(0.931)	0.169	**0.870**	0.094	0.066	0.191	0.218	-0.027	0.126
	0.161	**0.819**	0.149	-0.014	0.219	0.292	0.026	0.153
SV	0.169	0.158	**0.827**	0.221	0.170	0.151	−0.112	0.124
(0.926)	0.168	0.095	**0.852**	0.169	0.229	0.097	-0.151	-0.001
	0.210	0.148	**0.856**	0.216	0.109	0.146	-0.093	0.061
VU	−0.010	0.033	0.193	**0.932**	0.078	−0.016	−0.024	0.116
(0.942)	0.108	0.002	0.175	**0.929**	0.085	0.015	-0.050	0.018
	0.209	0.088	0.137	**0.899**	-0.007	0.079	0.031	0.095
RE	0.067	0.268	0.173	0.096	**0.782**	0.257	0.015	0.218
(0.898)	0.182	0.282	0.128	-0.019	**0.817**	0.163	-0.050	0.202
	0.178	0.138	0.215	0.105	**0.846**	0.072	-0.021	0.112
SE	0.196	0.176	0.181	0.011	0.162	**0.863**	0.034	0.154
(0.940)	0.266	0.209	0.123	0.045	0.129	**0.851**	0.008	0.116
	0.153	0.287	0.084	0.031	0.154	**0.859**	0.093	0.165
ICI	−0.012	−0.038	−0.148	−0.051	−0.030	0.082	**0.942**	0.021
(0.915)	-0.035	0.006	-0.105	0.013	-0.009	0.014	**0.957**	0.019
SDI	0.240	0.169	0.064	0.114	0.271	0.190	0.056	**0.856**
(0.948)	0.223	0.145	0.090	0.141	0.216	0.227	0.001	**0.869**

Table 6 Results of confirmatory factor analysis

Factor	Item	Factor loading	Error term	CR	AVE
SA	I know the potential security threat and its negative consequences.	0.905	0.456	0.853	0.659
	I understand the potential security threat and its negative consequences.	0.918	0.421		
	I have knowledge on the damage from potential security threat and its negative consequences.	0.899	0.399		
SS	I am satisfied with the effectiveness of security system of organization.	0.915	0.340	0.866	0.684
	I think the organization makes sufficient investment in security system.	0.886	0.393		
	I think the organization earmarks enough budgets for security system.	0.894	0.383		
SV	I think security threat on healthcare information is severe.	0.846	0.714	0.828	0.617
	I think it's severe a non-authorized party to access medical information.	0.926	0.345		
	I think the actions to attack (do damage to) healthcare information are serious.	0.907	0.422		
VU	I think healthcare information is vulnerable to security threat.	0.887	0.551	0.870	0.691
	I think the possibility is high that healthcare information is damaged by others.	0.935	0.303		
	I think the possibility is high that security threat on healthcare information is made at me.	0.936	0.277		
RE	I think efforts to prevent security threat on healthcare information are effective.	0.808	0.558	0.842	0.640
	I think countermeasures to prevent security threat on healthcare information are effective.	0.906	0.301		
	I think preventative measures to prevent others from using healthcare information I deal with are appropriate and relevant.	0.876	0.397		
SE	It's easy for me to take security measures on healthcare information.	0.935	0.344	0.856	0.666
	I know how to make security measures on healthcare information.	0.897	0.520		
	I have enough capability to prevent security threat on healthcare information.	0.916	0.397		
ICI	I have an intention of using other's ID without permit.	0.812	0.398	0.917	0.849
	I have an intention of using healthcare information illegally without authority.	1.039	−0.089		
SDI	I have an intention of configuring programs to control access for protecting healthcare information.	0.934	0.331	0.876	0.780
	I have an intention to set up programs to detect invasion for protecting healthcare information.	0.964	0.175		

Table 7 Correlation coefficient and AVE

	SA	SS	SV	VU	RE	SE	ICI	SDI
SA	0.659							
SS	0.512	0.684						
SV	0.554	0.416	0.617					
VU	0.322	0.158	0.450	0.691				
RE	0.505	0.614	0.480	0.195	0.640			
SE	0.557	0.587	0.388	0.124	0.502	0.666		
ICI	−0.067	−0.058	−0.257	−0.104	0.090	−0.073	0.849	
SDI	0.560	0.450	0.314	0.264	0.500	0.583	0.032	0.780

4.3 Research model analysis result

Since the reliability and validity of the constructs were verified by factor analysis, the goodness-of-fit of the research model was assessed. The results show the goodness-of-fit index includes χ2 (195, N = 222) = 446.125, $p < 0.000$, GFI = 0.851, CFI = 0.944, NFI = 0.906, TLI = 0.934, RMSE = 0.076. Although some of the values do not satisfy the conservative minimum requirement of 0.9, the goodness-of-fit of the research model is considered as reliable because the values are close to the conservative requirement and there is no absolute standard for the goodness-of-fit index. Additionally, the NFI, which represents the increment in fit of the hypothesized model relative to the null model, has a high value of 0.906; the CFI, which compares the null model with a hypothesized model that has no average or restriction, has a high value of 0.944; and the non-standardized TLI has a high value of 0.904; thus the model is comparatively fit. Therefore, the results of this research model are reliable.

Table 8 shows the result of each hypothesis derived by using structural equation. The path coefficients of hypothesis 1 are H1a (0.557, $p < 0.01$), H1b (0.107, unsupported), H1c (0.270, $p < 0.01$), and H1d (0.392, $p < 0.01$), showing that security awareness has significant influences on severity, response-efficacy, and self-efficacy. That is, the results indicate that in case the actual HIS users are clearly aware of the consequences of security threats, they will thoroughly understand the severity of the threats, and their response-efficacy and self-efficacy will be high because they pay much attention to healthcare information protection. On the other hand, security awareness does not have a significant influence on vulnerability, That is, although users feel that security threats may occur through their awareness of the consequences of security threats, they are not aware of that the security threat will occur to themselves. The path coefficients of hypothesis 2 are H2a (0.451, $p < 0.01$) and H2b (0.441, $p < 0.01$), suggesting that HIS users are satisfied with the security system; they trust in the responses to security threats and think that they can avoid actual security threats in case they recognize continuous investments on the security system. In other words, HIS user's trust in the security system and their familiarity with how to use it increases the response-efficacy and self-efficacy. The path coefficients of hypothesis 3 are H3a (0.390, $p < 0.01$), H3b (−0.315, $p < 0.01$), H3c (0.033, unsupported), and H3d (0.069, unsupported), indicating that the severity perceived by

Table 8 Analysis results of the hypotheses in the research model

	Path		Standardized path co-efficient	SE	CR	p	Result
	From	To					
H1a	SA	SV	0.557	0.067	8.250	0.000***	Supported
H1b	SA	VU	0.107	0.086	1.326	0.185	Not supported
H1c	SA	RE	0.270	0.051	3.776	0.000***	Supported
H1d	SA	SE	0.392	0.068	6.225	0.000***	Supported
H2a	SS	RE	0.451	0.051	5.916	0.000***	Supported
H2b	SS	SE	0.441	0.063	7.067	0.000***	Supported
H3a	SV	VU	0.390	0.089	4.745	0.000***	Supported
H3b	SV	ICI	−0.315	0.063	−3.502	0.000***	Supported
H3c	VU	ICI	0.033	0.049	0.430	0.667	Not supported
H3d	RE	ICI	0.069	0.069	0.971	0.331	Not supported
H4a	SE	RE	0.120	0.052	1.523	0.128	Not supported
H4b	VU	SDI	0.160	0.060	2.709	0.007***	Supported
H4c	RE	SDI	0.408	0.109	5.701	0.000***	Supported
H4d	SE	SDI	0.269	0.068	4.017	0.000***	Supported

*** $p < 0.01$, ** $p < 0.05$, *$p < 0.1$

HIS users has a significant influence on vulnerability and ICI of HIS users. These results imply that in case HIS users perceive severity through security awareness, they will recognize that security threats may occur to themselves. The path coefficients of hypothesis 4 are H4a (0.120, unsupported), H4b (0.160, $p < 0.01$), H4c (0.408, $p < 0.01$), and H4d (0.269, $p < 0.01$), demonstrating that if HIS users have the self-confidence that they can solve security threats by themselves, they do not trust in the security policy but instead form an intention to prevent security threats by themselves through severity, response-efficacy, and self-efficacy. That is to say, because SDI is formed through the coping appraisal when HIS users are satisfied with the security system and trust in the effect of actual security policy, investments on security system is very important for establishing a user-led healthcare information protection environment.

5 Discussion, implications and conclusion (Fig. 2)

Healthcare information is very sensitive because it may lead to secondary psychological damages to patients in case healthcare information leaks, and users' understanding on healthcare information protection is important because healthcare information leakage has been increasing continuously due to the low security awareness of HIS users. However, while previous studies on healthcare information protection mainly focused on the improvement of security policy and the function of security system, they failed to pay attention to HIPI of HIS users. Besides, because protection intention is formed by various appraisal antecedents, an integrated model that takes into consideration users' appraisal antecedents when HIPI is formed is required. Thus, this study put an emphasis on HIPI of HIS users and examined the implications of healthcare information protection. In other words, this study suggested an integrated model that utilizes GDT and PMT to identify which antecedents cause ICI and SDI of HIS users and what kinds of influence they will have on HIPI. Therefore, based on the idea that healthcare information leakage is mainly caused by HIS users, this study focused on the protection intention perceived by users and derived results that can help protect healthcare information more practically, which overcame the limitations of existing studies.

This study demonstrated that HIPI can be increased by users' clear awareness of the consequences of security threats, their satisfaction in the security system, and their self-efficacy that they can fully utilize the security system. First, no matter how elaborately the security policy has been established, if users are not clearly aware of the consequences of security threats, their severity of healthcare information leakage, satisfaction in security policy and self-efficacy will decrease. This implies that not only the security policy for the operation of HIS in each medical institution is important, but HIS users must also be clearly aware of the consequences of security threats. That is to say, it is necessary to make users understand the consequences of security threats more objectively through actual damage case-oriented education. Second, high

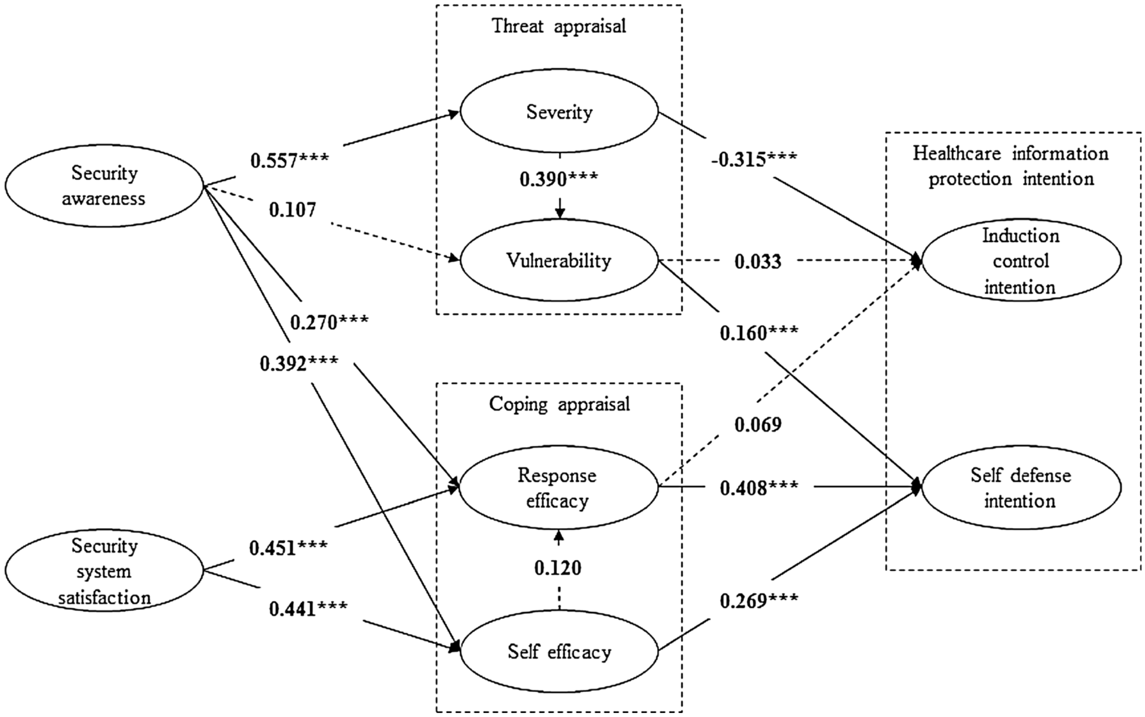

Fig. 2 Analysis results

satisfaction with the security system increases HIS users' self-confidence with healthcare information protection, leading to higher SDI of users. In other words, continuous investment on the security system is necessary, and the improved security system should be easier for HIS users to utilize. Furthermore, response-efficacy is the main factor of coping appraisal, triggering users motivation to participate in healthcare information protection, because satisfaction with the security system increases satisfaction in the effect of security policy. Finally, severity is the main antecedent of ICI, intention of HIS users to illegally use healthcare information, suggesting that although HIS users know much about the risks due to the consequences of security threats, they think that such risks will not occur to themselves in reality. Thus, it is essential to make HIS users clearly recognize the various threats and their responsibilities due to healthcare information leakage, as well as to make them recognize that they may be harmed by security threats anytime.

This study suggests the following strategies to increase HIPI of HIS users. First, efforts should be put on security education to make users clearly understand the security policy of HIS and recognize their responsibilities regarding the various threats and consequences due to healthcare information leakage. Since most of healthcare information leakages occurred were caused by the carelessness or abuse of HIS users, education for HIS users is very important in order to prevent healthcare information leakage in advance. Second, continuous investment on the security system is necessary in order to make HIS users use the security system easily. A direct factor to increase HIPI is the feeling of necessity of the security system by HIS users and their confidence on the security system to be used easily. That is to say, only if investments are made on the security system which takes users into consideration, HIS users' self-efficacy on healthcare information protection will be increased.

This study suggested that instead of security policy, clear awareness of the consequences of security threats and satisfaction with the security system are prerequisites to increase HIPI of HIS users. However, factors that have influences on HIPI are more extensive and HIS users belong to various occupational groups. Therefore, although this study classified the antecedents into security policy, security awareness, and security system using deterrence factors, if the users are classified into more categories based on their occupations or demographic characteristics, or more antecedents are included to explain the antecedents of HIPI more specifically, more concrete antecedents that have influences on HIPI could be found and strategies for increasing HIPI could be established more elaborately.

References

Agarwal, R., Gao, G. G., DesRoches, C., & Jha, A. K. (2010). Research commentary—the digital transformation of healthcare: current status and the road ahead. *Information Systems Research*, *21*, 796–809.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). *Security policy compliance: User acceptance perspective, system science (HICSS), 2012 45th Hawaii international conference on*. IEEE.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22*, 469–490.

Bønes, E., Hasvold, P., Henriksen, E., & Strandenæs, T. (2007). Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International Journal of Medical Informatics*, *76*, 677–687.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 523–556.

Caro, D. H. J. (2008). Deconstructing symbiotic dyadic e-health networks: transnational and transgenic perspectives. *International Journal of Information Management*, *28*, 94–101.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security*, *1*, 18–41.

Chang, I., Hwang, H. G., Hung, M. C., Kuo, K. M., & Yen, D. C. (2009). Factors affecting cross-hospital exchange of electronic medical records. *Information & Management*, *46*, 109–115.

Colling R.L., & York T.W. 2010 Electronic security system integration. Hospital and Healthcare Security (Fifth Edition)

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. *MIS Quarterly*, *19*, 189–211.

Crossler R.E. 2010. *Protection Motivation Theory*: *Understanding Determinants to Backing Up Personal Data*. System Sciences (HICSS), 2010 43rd Hawaii international conference on. IEEE.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*, *89*, 59–71.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*, 79–98.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the ACM*, *43*, 125–128.

Duan, L., Street, W. N., & Xu, E. (2011). Healthcare information systems: data mining methods in the creation of a clinical recommender system. *Enterprise Information Systems*, *5*, 169–181.

Edwards, W. (1954). The theory of decision making. *Psychological Bulletin*, *51*, 380–417.

GE. 2012. "Centricity Radiology Mobile Access." http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT/Medical_Imaging_Informatics_-_RIS-PACS-CVIS/Centricity_Radiology_Mobile_Access. Accessed Dec 2013.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems*, *13*, 29–48.

GOVTECH. 2012. "Utah CIO Steve Fletcher Resigns, State Promises Security Reforms." http://www.govtech.com/policy-management/Utah-CIO-Steve-Fletcher-Resigns-State-Promises-Security-Reforms.html Accessed Dec 2013.

Gritzalis, D., & Lambrinoudakis, C. (2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics*, *73*, 305–310.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, *20*, 257–278.

He, D. D., Yang, J., Compton, M., & Taylor, K. (2012). Authorization in cross-border eHealth systems. *Information Systems Frontiers*, *14*, 43–55.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*, 154–165.

HIMSS 2012. "HIMSS Annual Security Survey Results." Accessed Dec 2013. http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=280

Hupert, N., Lawthers, A. G., Brennan, T. A., & Peterson, L. M. (1996). Processing the tort deterrent signal: a qualitative study. *Social Science & Medicine*, *43*, 1–11.

Hurson, A., Ploskonka, J., Jiao, Y., & Haridas, H. (2004). Security issues and solutions in distributed heterogeneous mobile database systems. *Advances in Computers*, *61*, 107–198.

Ifinedo, P. (2011). Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*, 83–95.

ITRC. 2012. "2012 ITRC Breach Report." http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2012.shtml. Accessed Dec 2013.

Janczewski, L., & Xinli Shi, F. (2002). Development of information security baselines for healthcare information systems in New Zealand. *Computers & Security*, *21*, 172–192.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*, 549–566.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*, 139–154.

Kwok, L. F., & Longley, D. (1999). Information security management and modeling. *Information Management & Computer Security*, *7*, 30–39.

Law, K. C. K., Ip, H. H. S., & Chan, S. L. (1995). An investigation of a cost-effective solution for multimedia medical information management. *Information & Management*, *28*, 361–376.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*, 707–718.

Lluch, M. (2011). Healthcare professionals' organisational barriers to health information technologies—a literature review. *International Journal of Medical Informatics*, *80*, 849–862.

Lorence, D. P., & Spink, A. (2004). Healthcare information systems outsourcing. *International Journal of Information Management*, *24*, 131–145.

Milne, S., Sheeran, P., & Orbell, S. (2006). Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*, 106–143.

Mouttham, A., Kuziemsky, C., Langayan, D., Peyton, L., & Pereira, J. (2012). Interoperable support for collaborative, mobile, and accessible health care. *Information Systems Frontiers*, *14*, 73–85.

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

Poba-Nzaou, P., Uwizeyemungu, S., Raymond, L., & Paré, G. (2014). Motivations underlying the adoption of ERP systems in healthcare organizations: insights from online stories. *Information Systems Frontiers*, *16*, 591–605.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, *52*, 596–604.

Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. Social psychophysiology.

Siddiqui, Z., Abdullah, A. H., Khan, M. K., & Alghamdi, A. S. (2014). Smart environment as a service: three factor cloud based user authentication for telecare medical information system. *Journal of Medical Systems*, *38*, 1–14.

Siemens. 2012. "http://syngo.via." http://healthcare.siemens.com/medical-imaging-it/clinical-imaging-applications/syngovia. Accessed Dec 2013.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*, 31–41.

Straub Jr., D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly*, *14*, 45–60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *Management Information Systems Quarterly*, *22*, 441–470.

Teoh, S. Y., Pan, S. L., & Ramchand, A. M. (2012). Resource management activities in healthcare information systems: a process perspective. *Information Systems Frontiers*, *14*, 585–600.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*, 472–484.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*, 190–198.

Williams, F., & Boren, S. A. (2008). The role of the electronic medical record (EMR) in care delivery development in developing countries: a systematic review. *Informatics in Primary Care*, *16*, 139–145.

Woon, I., Tan, G.W., & Low, R. 2005 A protection motivation theory approach to home wireless security, ICIS 2005 proceedings

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, *24*, 2799–2816.

Wu, I. L., Li, J. Y., & Fu, C. Y. (2011). The adoption of mobile healthcare by hospital's professionals: an integrative perspective. *Decision Support Systems*, *51*, 587–596.

Yao, W., Chu, C.-H., & Li, Z. (2012). The adoption and implementation of RFID technologies in healthcare: a literature review. *Journal of Medical Systems*, *36*, 3507–3525.