Factors Influencing Attitudes Towards Patients' Personal Information Protection

Completed Research Paper

Shin-Yuan Hung **Annie Pei-I Yu**

Yu-Li Hung **Kuanchin Chen**

Hui-Ting Hung

Abstract

With the rapid development of information and communication technologies (ICT), many organizations engage in extensive ICT applications, resulting in a vast amount of personal data to be collected, processed and used. Consequently, the collected personal data is not always well-protected, a key reason for many recent data breaches. The aim of this study is to explore factors influencing the patient's attitude towards personal information protection. Based on the privacy calculus theory and technology threat avoidance theory, a research model was developed and several factors influencing the patient's attitude towards personal information protection were examined. A total of 423 usable responses were collected from a survey with the final response rate of 94.4%. The results indicated that perceived ease of use, legal assurance, privacy concerns and health information sensitivity positively affect the patient's attitude towards personal information protection. Finally, this study concluded with several useful recommendations for academics and practitioners.

Keyword: Personal information protection, personal information disclosure, healthcare information system service, privacy calculus theory, technology threat avoidance theory

Introduction

In recent years, personal information protection (IP) and information disclosure (ID) have received considerable attention from academics and practitioners (Pan et al. 2006; Culnan et al. 2009; Zimmer et al. 2010; Stulzman et al. 2011; Sharma et al. 2014). Nowadays, many forms of personal information about all aspect of daily human life are produced, collected, and processed via various IT techniques, causing a large-scale data stored and accessible in the cloud. Not surprisingly, personal information is considered to be the treasure of the digital age as the monetary value of the data can be estimated (Malgieri and Custers, 2018). Furthermore, the data have the potential to generate revenues and profits on its own (ENISA 2018). Personal information database can be decisive for the firms in the battle for market share. From the positive point of view, the fair use of the collected personal information benefits both the organizations and the general public. For example, the collection of patient records (e.g., e-medical records and telemedicine) for medical research which are important for improving medical services and healthcare (Watt 2006; Hartmann et al. 2019).

However, information technology is a double-edged sword. As stated earlier, advances in computer information technology improve human welfare, but problems arise such as security and privacy threats from hackers (Liang and Xue 2009; Fernandes et al. 2012), so personal information protection has become more and more important. At the same time, empowered individuals also are aware of the potential risks, would have more thoughts regarding how their personal information is collected and used (Beldad et al. 2012). Many studies on personal information focused on determents on disclosure and sharing, particularly to investigate factors influencing the willingness or intention, or the adoption (e.g., Beldad et al. 2012). In recent years, this issue has growing its importance for public health authorities (Weizman et al. 2012).

This paper mainly focused upon data protection in the context of healthcare. A healthcare organization's practice on information protection (IP) affects their patients' information disclosure (ID) intention in practice. Insufficient protection of personal data will affect the willingness of individuals to disclose personal information. However, as this sensitive personal information can be accessed via mobile devices, concerns about data ownership, privacy, and security to patient protection have motivated researchers to explore personal information protection and disclosure issues (Laric and Pitta2009; Medlin and Cazier 2010). The data sensitivity can lead to the general public refusal to disclose their information due to privacy and security concerns. In addition, patients are reported that the most mentioned objections to sharing data because they are afraid of suffering from discrimination by insurance companies (Weizman et al. 2012). In this paper, we intend to investigate the factors influencing the formation of "personal information protection" attitude and the moderating role of personal factor.

Although legislation have been enacted to regulate the scope of collection, processing, and use of personal information (such as the name, Id card number, medical record and treatment, genetic information, etc.), the emergence of new technology accelerates information retrieval, and transmission and circulation, intensifying an individual's concern of misuse of their personal data by a third party (Angst et al. 2010; Kapoor and Nazareth 2013). Previous studies have examined how the data protection policy of an organization influenced individuals' trust and their behavior, particularly in the context of electronic commerce or the use of social media (e.g., Pan et al. 2006; Stutzman et al. 2011), but little is known about patient attitudes toward information protection and data disclosure to medical services providers. The closer relationships between patients and healthcare providers as compared to the relationships between consumers and online vendors have set the healthcare environment apart from other contexts. As a result, construct relationships identified in previous studies in other contexts may not be readily applicable. Therefore, it is critical to explore the factors influencing the individual's attitude toward personal information protection and their associated risks. Thus, this study adopted the Technology Threat Avoidance Theory (TTAT) as well as Privacy Calculus Theory (PCT) to establish an attitude model named "Sensitive Medical Personal Information Exposure and Protection Attitude Model." This model provides a framework at an individual level. We theorize that two forces jointed drive patients' attitudes toward personal information protection-benefit and risk factors. On the one hand, patients may be more like to form a positive attitude toward personal information protection when

they perceived certain benefits would obtain such as rewards, perceived usefulness, and ease of use of systems and legal assurance from the healthcare providers to process their data. On the other hand, they may form a negative attitude towards personal information protection if they are concerned that negative results from the information system provided by healthcare service providers. Although Privacy Calculus Theory (PCT) has been applied in many adoption literature; it didn't not discuss the two forces at the same time. Additionally, TTAT was included in our model in order to include cognitive processes under threatening condition. The presented model is more suitable based on motivation theory. The paper addresses the following research questions:

1. How do perceived privacy risk and perceive benefits affect information protection attitudes?
2. How do TTAT and PCT affect the above relationships?
3. Whether do other personal factors moderate the influences on the formation of attitude?

Thus, our findings extend the recent literature providing a completed model to represent the determents of attitudes towards personal IP, reflecting users' concerns for information protection in the context of healthcare. The findings contribute to obtain deep understandings of patients' attitude and further their behavior, further to design effective communication strategy to change their attitude and behavior.

Literature Review

Studies Related to Personal Information Protection (IP) and Personal Information Disclosure (ID)

Personal information protection and disclosure are two sides of the same coin. Previous literature relating to personal information protection mainly focuses on changes in the legal system, norms and regulations, sources of personal data (clients or employees), or narrowing down the issues in specific areas such as financial risks, a particular government unit (Gandy 1993; Lenhart and Madden 2007; Phelps et al. 2000; Lansdale 1988; Milberg et al. 1995). In addition, existing studies relating to data protection have discussed the issue combining other legal regulations such as studies on laws, financial and technological management (Chellappa et al. 2002).

Another research stream focuses on how the companies' data protection policy (or privacy policy) affect consumers' attitude toward information disclosure intentions (Pan et al. 2006). In the context of online shopping Pan et al. (2006) found that the privacy policy of online stores would affect consumers' trust when perceived risk is high. Also, a short, straightforward privacy statement is easier for online consumers to understand than a lengthy legal privacy statement. Zimmer et al. (2010) presented the Information Disclosure Model based on Theory of Action and Transaction Cost Theory to examine factors influencing attitude towards online personal information disclosure and their impacts on intention. The findings showed that trust would reduce consumers' perceived risk and further positively affect their attitude and intention. Stutzman et al. (2011) discussed factors mediating disclosure in social networking sites. Their research further confirmed that Facebook users' attitude towards privacy and information disclosure would be controlled by Facebook privacy setting and policy statements. Sharma et al. (2014) found that individuals' the perceived usefulness of information disclosure during the transaction in social commerce would positively influence their intention while perceived risks would negatively affect the intention of the disclosure. Li et al. (2015) found the role of gender and age on information disclosure behavior. These studies show the behavior of personal information disclosure under online transactions or social media. These studies of information protection and disclosure in online contexts provide some preliminary research findings. However, the sensitivity of the information people disclosure for social interaction is different from for shopping; furthermore, is far different from for medical and healthcare services. In addition, little is known in terms of protection and avoidance to potential threats (Culnan 1993; Smith 1993; Liang and Xue 2009; Liang and Xue 2010; Adjerid et al. 2015). Xu et al. (2011) argue that personal information protection is influenced by multiple factors, including information exchange, a social construct, and information control. The current research aims at closing the research gap to amend the weakness of previous studies.

Privacy Calculus Theory

Privacy calculus theory refers to an individual's intention to disclose personal information based on the consideration between risk-taking and benefits receiving (Culnan and Armstrong 1999). According to this theory, people are afraid of losing their privacy for security concerns but also delightful to expect to obtain more benefits from personalized services. The phenomenon is called privacy paradox. If an individual realizes more benefits would obtain for sharing their personal information to the marketers and believe their personal information would be reasonably used, they are more likely to disclose their personal information (Gutierrez et al. 2018). Privacy calculus theory has been widely used in explaining individuals' personal information disclosing behavior, particularly with the development of technology in social media and e-commerce (Gutierrez et al. 2018). For example, many retailers collect consumers' data via the customer membership scheme. Based on the database, retailers can analyze and predict consumers' needs. Recently, companies develop mobile apps and use the GPS technique to collect consumers' location data. Send location-based advertisement and promotion messages to attract consumers' attention to shop (Gutierrez et al. 2018). Individuals agree to join the customer membership scheme, installing the apps on their mobile phone and registering a membership account because they believe the benefits they get (e.g., special offers, incentives, or cash back) more than the cost they lose (Dinev et al. 2006; Li et al. 2010; Xu et al. 2011; Kehr et al. 2015; Njenga and Ndlovu 2012). In other words, privacy means an individual believes they are capable and aware of the data use under their control (Hann et al. 2007). With the development of social media and mobile devices, individuals tend to get used to sharing certain personal information for particular social internal purposes. However, they are not familiar if their data are used in the context of healthcare or medical services. It is difficult to calculate the cost to disclose personal data and perceived potential benefits get from healthcare organizations. To sum up, the perception of privacy risk and concern is hard to calculate its monetary value but normally by individuals' subjective judgment.

Technology Threat Avoidance Theory

Technology threat avoidance theory (TTAT), proposed by Liang and Xue (2009), is used to explain individual IT users' avoidance behavior toward the threats of technology. According to the TTAT, users' avoidance behavior is based on their perception by evaluating the effectiveness and costs of the technology. Users tend to avoid a particular technology application when they perceive a threat to obtaining personal security. Although technology acceptance theory (TAM) tells us why people are willing to adopt new technology, TTAT further explains why people refrain from certain technology services (Carver and White 1994; Elliot 2006; Elliot and Covington 2001). This theory argues that one's adoption and avoidance behavior is different. People tend to approach positive events and avoid negative events (Elliot 2006), which is called Approach-Avoidance conflicts. In the context of healthcare and medical services, shared personal information and data may bring positive feedback but also has the potential to bring negative results. In other words, positive events include better medical and convenience medial healthcare services, but negative events may include privacy fraud. Liang and Xue (2009) proposed the threat perception is shaped by two antecedents: perceived susceptibility and perceived severity. Perceived susceptibility refers to people's subjective perception that the state of being easy affected, and perceived severity means the extent to which a human being perceives that negative results caused by the harmful IT are severe.

Research Model

Rooted in the privacy calculus theory and technology threat avoidance theory, our research model includes three dimensions: benefit factors, risk factors and personal factors to explore the critical factors influencing the patient's attitude towards personal information protection are examined. Figure 1 shows our research model.

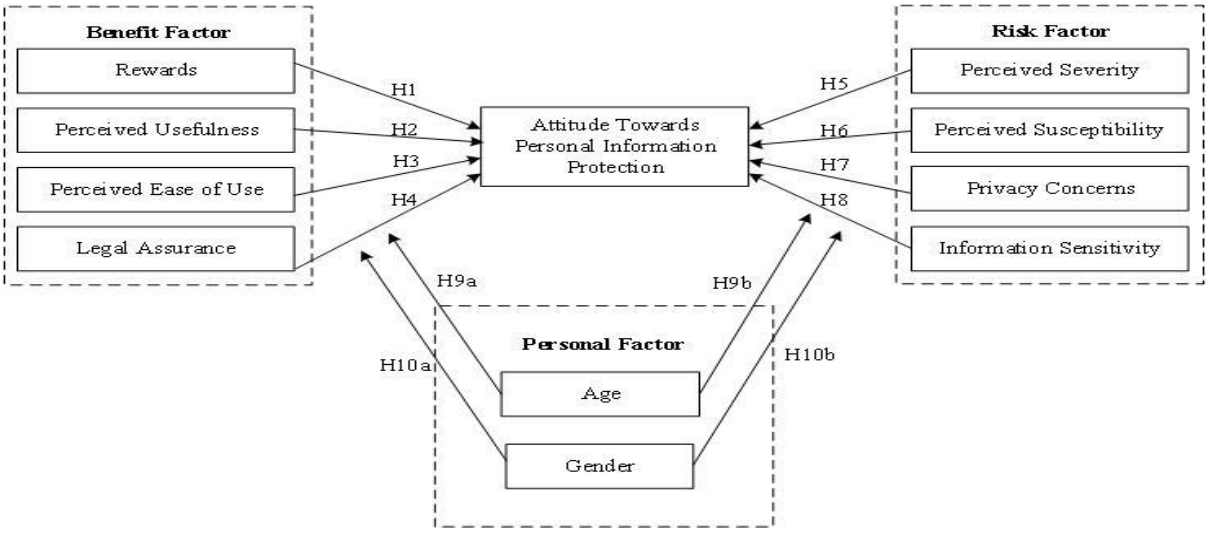

Figure 1. Research Model

Research Hypotheses

Rewards, perceived usefulness and perceived ease of use of information technology have different influences on the patient's attitude towards personal information protection.

The PMT (Protection Motivation Theory) proposed by Roger in 1975 explains how people respond to potential threats and assesses their ability when perceived threatening events are happening. The "reward" factor was later added to PMT in 1983 to denote variations of people's response to threats when rewards and incentives are present.

Technology threat avoidance theory developed base on PMT's threat appraisal and coping appraisal by Liang et al. (2009). Liang et al. (2010) pointed out that the perceived usefulness of information technology will help users to adopt information technology. The perceived ease of use of information technology was affected by the degree of data privacy. For example, benefits or rewards resulted from using electronic medical records is better healthcare services. Dinev et al. (2006) pointed out that personal benefit and trust website will increase user willingness to disclose their information; Njenga et al. (2012) indicated that perceived usefulness and perceived ease of use have a direct effect on perceived benefit of information technology; Kehr et al. (2015) pointed out that perceived ease of use of information technology have a direct effect on attitude toward information disclosure after privacy calculus. According to the discussion above, this study proposed the following hypotheses:

H1: Rewards or benefits provided by healthcare information services have a positive effect on the patient's attitude towards personal information protection.

H2: Perceived usefulness of healthcare information services has a positive effect on the patient's attitude towards personal information protection.

H3: Perceived ease of use of healthcare information services have a positive effect on the patient's attitude towards personal information protection.

Personal data and legal assurance of medical have different influences on attitude towards personal information protection.

There is still a sustaining interest in privacy calculus to explore factors such as legal assurance. Li et al. (2010) used fair exchange as the model antecedent to explain exchange benefit, and privacy costs have different influences on behavior intention. Krasonva et al. (2010) pointed out that personal benefit and trust website have a direct effect on self-disclosure. Kehr et al. (2015) indicated that organizational trust

includes legal assurance. The legal assurance has a direct effect on Intentions to disclose. Therefore, this study proposal Hypotheses 4.

H4: Legal assurance of healthcare information services has a positive effect on the patient's attitude towards personal information protection.

Perceived severity and perceived susceptibility of information technology have different influences on the patient's attitude towards personal information protection.

Rogers (1975), Maddux and Rogers (1983) and Liang et al. (2009) pointed out that the risks of information technology can be used to assess potential threat. The perceived severity refers to the negative consequences an individual associated with an event or outcome. These consequences may relate to an anticipated event that may occur in the future, or to a current state. The perceived susceptibility refers to one's perception of the risk or the chances of contracting the threat of attack. As such susceptibility raises a red flag in an individual's assessment of their reaction to threat, it affects their attitudes towards personal information protection. Therefore, this study proposal Hypotheses 5 and 6.

H5: Perceived severity of threat to healthcare information services has a negative effect on the patient's attitude towards personal information protection.

H6: Perceived susceptibility of threat to healthcare information services has a negative effect on the patient's attitude towards personal information protection.

Privacy concerns are arising from the provision of highly sensitive medical information by individuals.

Dinev and Hart (2004, 2006) pointed out that the perceived weakness or perceived ability of information technology have an effect on privacy concerns, changes the willingness to disclose information, and adds perceived risk. Krasonva et al. (2010) used the perceived likelihood and perceived risk of information technology to infer the privacy concern's factor. Xu et al. (2011) indicated that the personalization and privacy risk had a significant influence on privacy concerns. Based on the above discussion, prior studies have provided support for the privacy concerns of risk factors. Thus, we suggest the following hypotheses:

H7: Privacy concerns have a negative effect on the patient's attitude towards personal information protection.

Information sensitivity

Medical information is highly sensitive. Therefore, the Personal Data Protection Act has classified this information with special data. Kehr et al. (2015) pointed out that the characteristic of data (such as medical diagnosis results, medical records) will affect potential risks and potential benefits, and then affect user willingness to disclose their information. However, this study reviewed that other scholars pointed out the people react to privacy threats depend on the environment and the data type. Therefore, this study proposal Hypotheses 8.

H8: Information sensitivity has a negative effect on the patient's attitude towards personal information protection.

Age and gender of information technology have moderating influences on the patient's attitude toward personal information protection.

Previous studies indicated that gender, age, personal emotions, and rational or emotional personality had influenced privacy protection (Culnan and Armstrong 1999; Li et al. 2010; Xu et al. 2011; Kehr et al. 2015). The differences in demographics between age and gender have different opinions on the privacy of personal data (Li et al. 2010). Elias et al. (2012) pointed out that age had a different

moderating influence on information technology. Amit Kapoor (2015) indicated that the differences in demographics between age and gender have different opinions on the risk beliefs. Thus, we suggest the following hypotheses:

(1) Patient of different ages has a moderating effect on the patient's attitude towards personal information protection.

H9a: Benefit factors (rewards, perceived usefulness, perceived ease of use and legal assurance) of different ages have a moderating effect on the patient's attitude towards personal information protection.

H9b: Risk factors (perceived severity, perceived susceptibility, privacy concerns, and information sensitivity) of different ages have a moderating effect on the patient's attitude towards personal information protection.

(2) Patient of different gender has a moderating effect on the patient's attitude towards personal information protection

H10a: Benefit factors (rewards, perceived usefulness, perceived ease of use and legal assurance) of different gender have a moderating effect on the patient's attitude towards personal information protection.

H10b: Risk factors (perceived severity, perceived susceptibility, privacy concerns, and information sensitivity) of different gender have a moderating effect on the patient's attitude towards personal information protection.

RESEARCH METHOD

Questionnaire Development

This study adopted a questionnaire survey to collect data. In terms of scale design, all measures of each construct in Figure 1 were adopted from prior studies and were measured using a seven-point Likert scale. Although scale items had been validated by previous studies, we examined them to ensure that the content validity and reliability were within an acceptable range. We conducted pretests by requesting several healthcare information management or information management professors and Ph.D. students to evaluate the scale items. To ensure validity and reliability, we conducted a pilot test by requesting 20 to 30 the healthcare information management or information management experts. Table 1 presents the operational definition of variables, sources.

Table 1: Construct of Definitions and Sources

Construct	Operational definition	Reference
Rewards	Additional benefits (e.g., time and monetary efficiencies, and healthcare services or information offerings) patients will receive from using the healthcare information system.	Dinev et al. (2013)
Perceived Usefulness	The extent to which an individual perceives that useful and expected benefits obtained (e.g., quick and timely healthcare services) from the functions of healthcare information systems.	Davis (1989)
Perceived Ease of Use	The extent to which an individual perceives that friendly and easy to operate from the functions of healthcare information systems (e.g., user friendly healthcare service tools).	Davis (1989)
Legal Assurance	The degree to which an individual perceives that legal assurance about personal data in	Krasonova et al. (2010)

	the healthcare information systems (e.g., mechanisms for personal data abuse control and protection.).	
Perceived Severity	The extent to which an individual perceives that negative consequences regarding personal data disclosure caused by the healthcare information systems (e.g., privacy invasion and unauthorized secondary use).	Liang et al. (2010)
Perceived Susceptibility	An individual's subjective probability that the healthcare information system will negatively affect him or her.	Liang et al.(2010)
Privacy Concerns	The degree of concern (e.g., the threat of personal privacy in healthcare service tools) about personal data with the healthcare information systems from a subjective perspective.	Dinev et al.(2006) and Krasonova et al.(2010)
Information Sensitivity	The impact of different types of medical information systems on protection attitudes.	Bansal et al.(2010)
Attitude towards personal information protection	The patient's attitude towards the protection of their information by medical institutions.	Schwaig et al.(2013)

Sample and Data Collection

Subject were selected from those who had medical experience in Taiwan. To ensure the sample representativeness, this study uses the quota sampling method, using public information released by the Ministry of Health and Welfare to decide the number of intended respondents for each region of Taiwan to ensure that the sample distribution matches the reality. The number of intended respondents is determined based on the proportion of declared medical services points rendered by medical services institutions across various regions. That is, a survey lasting three months was carried out in North, Central, and South of Taiwan respectively. Incentives (coffee vouchers) were used to encourage the respondents to fill in the questionnaire attentively and to increase the completion rates. After respondents finished the survey, our research assistants checked the completion of the questions and started a quick conversation to gather respondents' thoughts of personal information disclosure. A total of 448 respondents participated in the survey. 25 samples were removed due to the incompletion. Thus, 423 respondents were involved in this study resulting in an effective response rate of 94.4%.

RESEARCH RESULT

Respondent Characteristics

The subjects in our survey had medical experience and had used at least one or more forms of healthcare service tools from our list. (i.e., My Health Bank, hospital app, online appointment system and automatic appointment machine). The demographic distribution is reported in Table 2 below.

Table 2. Respondent Demographics

Characteristics	Item	Frequency	Percentage
Gender	Male	183	43.3
	Female	240	56.7
Age	Under 19	8	1.9
	20-29	142	33.6
	30-39	120	28.4
	40-49	81	19.1
	50-59	54	12.8

	Over 60	18	4.3
Education	High school	52	12.3
	University/College	253	59.8
	Graduate school	118	27.9
Resident	Keelung/Taipei/New Taipei	212	50.1
	Taoyuan/Hsinchu/Miaoli	46	10.9
	Taichung/Changhua	100	23.6
	Yunlin/Chiayi/Tainan	18	4.3
	Kaohsiung/Pingtung	36	8.5
	Hualien/Taitung	7	1.7
Healthcare information service types	My Health Bank	3	0.7
	Hospital App	18	4.3
	Online Appointment System or Automatic Appointment Machine	316	74.7
	My Health Bank, Online Appointment System or Automatic Appointment Machine	7	1.7
	Hospital App, Online Appointment System or Automatic Appointment Machine	74	17.5
	All of the above are used	5	1.2

Reliability and Validity Analysis

This study used Cronbach's α to measure the reliability of constructs. Hair et al. (2006) pointed out that the value of Cronbach's α should be higher than 0.7. Our results show that Cronbach's α ranged from 0.703 to 0.967. We used the principal component analysis (PCA) to measure the construct validity. According to Hair (2006), the value of factor loadings should exceed 0.45. All our factor loadings ranged from 0.607 to 0.931. These results pointed out that the reliability of constructs and construct validity were at an acceptable level.

Multiple Regression Analysis

This study considers gender and age as moderator variables to explore independent variables (rewards, perceived usefulness, perceived ease of use, perceived severity, perceived susceptibility, privacy concerns, and information sensitivity) the relationship of the personal data protects have interference effects between different attitudes. Variables that have a negative effect (benefit factors) and positive effect (risk factors) were entered to the equation to predict the patient's attitude towards personal information protection. Results showed that perceived ease of use, legal assurance privacy concerns, and information sensitivity had a significant influence on the patient's attitude towards personal information protection. Table 3 showed the multiple regression analysis.

Table 3. Multiple Regression Analysis

Mode	Standardized Coefficients	P-value
Constant		0.004
Rewards	0.103	0.194
Perceived Usefulness	0.013	0.881
Perceived Ease of Use	0.121	0.054*
Legal Assurance	0.318	0.000***
Perceived Severity	0.014	0.843
Perceived Susceptibility	-0.020	0.776
Privacy Concerns	0.366	0.000***
Information Sensitivity	0.173	0.000***

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

The personal factor of the moderator effect

The study used Moderated Regression Analysis (MRA) to explore the different influences on the patient's attitude towards personal information protection. Two demographic variables (age and gender) were used to analyze the interaction between the independent variables and the dependent variable. Table 4 shows that the relationship between perceived ease of use and information sensitivity on the patient's attitude towards personal information protection moderated by the patient's age. Table 5 shows that the influence of perceived ease of use on the patient's attitude towards personal information protection moderated by the patient's gender.

Table 4. Two Groups Compared by Age

Mode		Standardized Coefficients	P-Value
≦30-39 (n=270)	Constant		0.029
	Perceived Ease of Use	0.199	0.001***
	Legal Assurance	0.143	0.032**
	Privacy Concerns	0.203	0.002***
	Information Sensitivity	0.253	0.000***
＞30-39 (n=153)	Constant		0.029
	Perceived Ease of Use	0.069	0.362
	Legal Assurance	0.352	0.000***
	Privacy Concerns	0.194	0.026**
	Information Sensitivity	0.043	0.554

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

Table 5. Two Groups Compared by Gender

Mode		Standardized Coefficients	P-Value
Male (n=183)	Constant		0.001
	Perceived Ease of Use	0.044	0.529
	Legal Assurance	0.223	0.008***
	Privacy Concerns	0.258	0.002***
	Information Sensitivity	0.245	0.000***
Female (n=240)	Constant		0.064*
	Perceived Ease of Use	0.226	0.001***
	Legal Assurance	0.219	0.002***
	Privacy Concerns	0.139	0.047**
	Information Sensitivity	0.105	0.070*

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

DISCUSSION

1. Benefit Factor

   Our results show that rewards and perceived usefulness did not have a statistical effect on patient's personal data protection. Upon further investigation of the data, we discovered that patients did not fully utilize the full range of features available on health providers' web sites or apps. The primary use heavily leaned towards online appointments and automatic appointment reminders (74.7%). Only about 5% respondents had used the healthcare provider's APP or My Health Bank. As a result, patients did not experience the full benefits provided by the available technology. Therefore, the reward and perceived usefulness did not affect the intention to protect personal data.

   The results showed that perceived ease of use had a positive and significant influence on the patient's attitude towards personal information protection. This is consistent with the results of Davis (1989). Our study showed that patients' ease of operations for automatic appointment

machine, online appointment system, hospital app, and My Health Bank are the main reasons for their willingness to adopt, and thus affect the extent to which personal data was provided.

Legal assurance had a positive influence on the patient's attitude towards personal information protection, showing patients' trust on the legislative enforcements to protect their personal information.

2. Risk Factor

   The results show that perceived severity and perceived susceptibility of healthcare information services did not influence the patient's attitude towards personal information protection, but privacy concerns outweigh other independent variables as the most influential variable on the patient's attitude towards personal information protection. The nature of the personal data itself is also a key predictor of the patient's attitude showing that protection intention varies across three pillars, including the information itself (i.e., information sensitivity), the patient's attitude (i.e., privacy concerns) and external assurance (i.e., legal assurance).

3. Personal Factor

   This study employed two demographic variables (age and gender) to analyze whether the significance among construct relationships still exists. The results include the following:

   (1) The patient's age had a moderating effect on perceived ease of use and information sensitivity.

   (2) The patient's gender had a moderating effect on perceived ease of use.

   Based on the above results, demographic factors had an interaction effect on the relationships between independent variables and the dependent variable. Therefore, this result confirmed the moderation role of patient's demographics.

Limitations and Conclusion

In this study, our research model was built on the privacy calculus theory and technology threat avoidance theory. The results of this study provide government agencies with advice on how to develop comprehensive information privacy protection goals. We demonstrated that the key predictors on attitudes towards personal information protection were: perceived ease of use, legal assurance, privacy concerns, and health information sensitivity. The benefit factors of legal assurance have become the most critical factor affecting patient's attitude towards personal information protection. If the hospital provides a clear and understandable data protection declaration, the patient tends to feel at ease and form a positive attitude of protection when they are requested to give their personal data to the hospital. In addition, the patient perception of the medical institution's information system is user-friendly, encouraging them to use healthcare service tools. It would ensure patients that their data keep in safe and increase their willingness to disclose more accurate personal data in details.

In addition, medical information is special data, which is more sensitive and highly transparent. This study indicated that patients are more likely to have privacy concerns when providing personal information to medical institutions, which in turn makes the information provided incomplete or incorrect. Therefore, regarding the collection, processing, and access to medical types, people will be more likely to have their own protection awareness. Furthermore, the medical industry or other developers should promote the medical information system should be formulated, explained and managed from the perspective of the public, so that the public can feel at ease when using it.

However, this study is not without limitations. First, this study adopted a cross-sectional study to investigate the research questions. Second, most of the respondents come from Taiwan. It is not appropriate to generalize from the findings to other countries. Although rewards, perceived usefulness, perceived severity, and perceived susceptibility may be less salient to predicting a patient's attitude towards personal information protection. We provide some insights for the academic scholars and practitioners based on our findings. We hope that this study will start up future interest in exploring the factors influencing the patients' attitude towards information protection and disclosure. In addition, we recommend that future study adopt a longitudinal study to obtain more deep understandings.

References

Adjerid, I., Acquisti, A., Telang, R., Padman, R., and Adler-Milstein, J. 2015. "The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges," *Management Science* (62:4), pp. 1042-1063.

Amit Kapoor. 2015. "Gender Differences In Risk Taking: Evidence From A Management Institute," *Journal of Advances in Business Management* (1), pp.1-5.

Angst, C. M., Agarwal, R., Sambamurthy, V., and Kelley, K. 2010. "Social Contagion And Information Technology Diffusion: The Adoption Of Electronic Medical Records In US Hospitals," *Management Science* (56:8), pp. 1219-1241.

Bansal, G., and Gefen, D. 2010. "The Impact Of Personal Dispositions On Information Sensitivity, Privacy Concern And Trust In Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138-150.

Beldad, A., van der Geest, T., de Jong, M., and Steehouder, M. 2012. "Shall I Tell You Where I Live and Who I Am? Factors Influencing the Behavioral Intention to Disclose Personal Data for Online Government Transactions," *International Journal of Human-Computer Interaction* (28:3), pp. 163-177. (https://doi.org/10.1080/10447318.2011.572331).

Carver, C. S., and White, T. L. 1994. "Behavioral Inhibition, Behavioral Activation, and Affective Responses to Impending Reward and Punishment: The BIS/BAS Scales," *Journal of Personality and Social Psychology* (67), pp. 319-333.

Chellappa, R. K., and Pavlou, P. A. 2002. "Perceived Information Security, Financial Liability And Consumer Trust In Electronic Commerce Transactions," *Logistics Information Management* (15:5/6), pp. 358-368.

Culnan, M. J. 1993. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (17:3), pp. 341-363.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, And Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Culnan, M. J., and Williams, C. C. 2009. "How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches," *MIS Quarterly* (33:4), pp. 673-687.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease Of Use, And User Acceptance Of Information Technolog," *MIS Quarterly* (13:3), pp. 319-340.

Dinev, T., and Hart, P. 2004. "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behaviour and Information Technology* (23:6), pp. 413-422.

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Dinev, T., Xu, H., Smith, J. H., and Hart, P. 2013. "Information Privacy And Correlates: An Empirical Attempt To Bridge And Distinguish Privacy-Related Concepts," *European Journal of Information Systems* (22:3), pp. 295-316.

Elias, S. M., Smith, W. L., and Barney, C. E. 2012. "Age as a moderator of attitude towards technology in the workplace: work motivation and overall job satisfaction," *Behaviour and Information Technology* (31:5), pp. 453-467.

European Union Agency for Network and Information Security, "The Value of Personal Online Data" [Cyber Security Info Notes], 2018. Data retrieved https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data.

Elliot, A. J. 2006. "The Hierarchical Model of Approach–Avoidance Motivation," *Motivation and Emotion* (30:2), pp.111-116.

Elliot, A. J., and Covington, M. V. 2001. "Approach and Avoidance Motivation," *Educational Psychology Review* (13:2), pp. 73-92.

Fernandes, L. M., O'Connor, M., and Weaver, V. 2012. "Big data, bigger outcomes," *Journal of AHIMA* (83:10), pp. 38-43.

Gandy Jr, O. H. (1993). Toward A Political Economy Of Personal Information. *Critical Studies in Media Communication* (10:1), pp. 70-97.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., and Calle, T. 2018. "Using Privacy Calculus Theory To Explore Entrepreneurial Directions In Mobile Location-Based Advertising: Identifying

Intrusiveness As The Critical Risk Factor," *Computers in Human Behavior*. doi:10.1016/j.chb.2018.09.015

Hair, J. F., Tatham, R. L., Anderson, R. E., and Black, W. 2006. *Multivariate data analysis* (Vol. 6). Upper Saddle River, NJ: Pearson Prentice Hall.

Hartmann, R., Sander, C., Lorenz, N., Böttger, D., and Hegerl, U. 2019. "Utilization of Patient-Generated Data Collected Through Mobile Devices: Insights From a Survey on Attitudes Toward Mobile Self-Monitoring and Self-Management Apps for Depression.," *JMIR Mental Health* (6:4), p. e11671. (https://doi.org/10.2196/11671).

Hann, H. I., Hui K. L., Lee S. Y. T., and Png, I.P.L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), pp.13-42.

Kapoor, A., and Nazareth, D. L. 2013. "Medical Data Breaches: What The Reported Data Illustrates, And Implications For Transitioning To Electronic Medical Records," *Journal of Applied Security Research* (8:1), pp. 61-79.

Kehr, F., Kowatsch, T., Wentzel, D., and Fleisch, E. 2015. "Blissfully Ignorant: The Effects Of General Privacy Concerns, General Institutional Trust, And Affect In The Privacy Calculus," *Information Systems Journal* (25:6), pp. 607-635.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109-125.

Lansdale, M. W. 1988. "The psychology of personal information management," *Applied Ergonomics* (19:1), pp. 55-66.

Laric, M. V., and Pitta, D. A. 2009. "Preserving Patient Privacy In The Quest For Health Care Economies," *Journal of Consumer Marketing* (26:7), pp. 477-486.

Lenhart, A., and Madden, M. 2007. "Teens, privacy and online social networks: How teens manage their online identities and personal information," The Age of MySpace Pew Internet and American Life Project, pp.45.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding Compliance With Internet Use Policy From The Perspective Of Rational Choice Theory," *Decision Support Systems* (48:4), pp. 635-645.

Li, K., Lin, Z., and Wang, X. 2015. "An empirical analysis of users' privacy disclosure behaviors on social network sites," *Information and management* (52:7), pp. 882-891.

Liang, H., and Xue, Y. 2009. "Avoidance Of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71-90.

Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors In Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems* (11:7), pp. 394-413.

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation And Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Malgieri, G., and Custers, B. 2018. "Pricing privacy–the right to know the value of your personal data," *Computer Law & Security Review* (34:2), pp. 289-303.

Medlin, B. D., and Cazier, J. 2010. "Obtaining Patient'S Information From Hospital Employees Through Social Engineering Techniques: An Investigative Study," in H. Nemati (Ed.), *Pervasive Information Security and Privacy Developments: Trends and Advancements: Trends and Advancements*, Hershey, PA: IGI Global, pp.77-89

Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. 1995. "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM* (38:12), pp. 65-74.

Njenga, K., and Ndlovu, S. 2012. "On Privacy Calculus And Underlying Consumer Concerns Influencing Mobile Banking Subscriptions," In *2012 Information Security for South Africa* (pp. 1–9). IEEE. http://doi.org/10.1109/ISSA.2012.6320453

Pan, Y., and Zinkhan, G. M. 2006. "Exploring the impact of online privacy disclosures on consumer trust," *Journal of Retailing* (82:4), pp. 331-338.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns And Consumer Willingness To Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp. 27-41.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology*, (91:1), pp. 93-114.

Schwaig, K. S., Segars, A. H., Grover, V., and Fiedler, K. D. 2013. "A model of consumers' perceptions of the invasion of information privacy," *Information and Management* (50:1), pp. 1-12.

Sharma, S., and Crossler, R. E. 2014. "Disclosing too much? Situational factors affecting information disclosure in social commerce environment," *Electronic Commerce Research and Applications* (13:5), pp. 305-319.

Smith, H.J. 1993. "Privacy Policies And Practices：Inside The Organizational Maze," *Communications of the ACM* (36:12), pp. 104-122.

Stutzman, F., Capra, R., and Thompson, J. 2011. "Factors mediating disclosure in social network sites," *Computers in Human Behavior* (27:1), pp. 590-598.

Watt, G. 2006. "Using Patient Records For Medical Research, *British Journal of General Practice*, 56(529), pp. 630-631.

Weitzman, E. R., Kelemen, S., Kaci, L., and Mandl, K. D. 2012. "Willingness to Share Personal Health Record Data for Care Improvement and Public Health: A Survey of Experienced Personal Health Record Users," *BMC Medical Informatics and Decision Making* (12:1), pp. 39. (https://doi.org/10.1186/1472-6947-12-39).

Xu, H., Luo, X. R., Carroll, J. M., and Rosson, M. B. 2011. "The Personalization Privacy Paradox: An Exploratory Study Of Decision Making Process For Location-Aware Marketing," *Decision Support Systems* (51:1), pp. 42-52.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., and Grover, V. 2010. "Investigating Online Information Disclosure: Effects Of Information Relevance, Trust And Risk," *Information and Management* (47:2), pp. 115-123.