An Assessment of Privacy Concerns on Personal Health Information: Thailand Case Study

Charnsak Srisawatsakul and Waransanang Boontarig*

Faculty of Computer Science, Ubon Ratchathani Rajabhat University,
Ubon Ratchathani, Thailand

Received: 21 January 2021, Revised: 2 April 2021, Accepted: 6 May 2021

Abstract

One of the most important industries that transforms into digital infrastructure is healthcare. Most healthcare organizations worldwide collect and process personal health information digitally. Personal health information is considered highly sensitive information. Hence, the increased collection of health information has raised concerns throughout society regarding potential privacy issues. Therefore, previous research paid attention to the study of privacy of health information in several contexts. In Thailand, Thai people are becoming more aware of privacy concerns than ever before. The reason is that the personal data protection act will become effective in May 2021. Hence, this study aims to understand the privacy concerns and behavioral intention to reveal Thais' personal health information. In this paper, we applied the Internet Users' Information Privacy Concerns model to the health information context. We collected data using an online questionnaire. The population consisted of Thai people who shared personal health information with the healthcare industry. The participants in this research were selected by the accidental sampling method. There were 84 participants in Thailand who were employed in the hypotheses testing using the linear regression equations. This study shows that personal health information collection and awareness directly influence personal health information privacy concerns. Furthermore, trusting belief is a factor that affects people's behavioral intention to share health information. The findings should help the healthcare industry to better understand the patients, so that they will offer their information willingly.

Keywords: GDPR; health information; IUIPC; PDPA; privacy concern; privacy
DOI........................

1. Introduction

Over the past decade, privacy concerns of personal information have been increasing around the world. The large-scale breach of personal information is the main reason that has accelerated the debate on how much personal information should be accessible by other entities, either private or government organizations. Organizations that store and process personal data need to be concerned about their privacy policies, and this is required by law in various parts of the world. The European

*Corresponding author: Tel.: (+66) 061-0509991
E-mail: waransanang.s@ubru.ac.th

Union (EU) employed the General Data Protection Regulation (GDPR) for the protection of personal data across European countries [1, 2]. The aim of GDPR was to protect personal data and ensure that it was processed securely. In Thailand, the government announced a new privacy law, which was the Personal Data Protection Act (PDPA) [3]. The government published PDPA in the Government Gazette on 27 May 2019. However, there is a grace period of 2 years before all of the act becomes effective. It has a similar purpose to GDPR, which is to protect the privacy of personal data.

Personal health information refers to medical histories, laboratory results, demographic information, mental and physical health conditions, insurance information, and any form of information that a healthcare professional collects to identify an individual and determine appropriate care [4]. It is considered one of the most sensitive forms of information, according to GDPR [5] and PDPA [3]. Furthermore, the healthcare industry has adopted numerous information technologies to digitize patients' health information, such as EMR (Electronic Medical Record). To date, the volume of personal health information collected in electronic form has continued to increase at exponential rates. Therefore, the privacy of personal health information is a vital concern of the industry.

Throughout the past decade, personal information privacy has become an increasingly interesting topic among researchers worldwide. However, there is still a lag of research on privacy concerns of personal health information in Thailand. Moreover, Thais are less concerned with the confidentiality and privacy of their information [6]. Hence, this prospective study investigates Thai people's privacy concerns in the personal health information context. This study's empirical research approach was adapted from the Internet Users' Information Privacy Concerns (IUIPC)[7].

2. Materials and Methods

2.1 Privacy

Nowadays, the GDPR defines the privacy of data as "empowering your users to make their own decisions about who can process their data and for what purpose" Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. However, privacy can be interpreted differently in various circumstances. Previous researchers have described it as dynamic, elastic, and multidimensional in the perception that it varies with life experience [8]. Solove [9] suggested that privacy can be classified as "(1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy". Likewise, Margulis [10] believes that the psychological concept subsumes a wide variety of privacy meanings. Privacy in the previous literature often focuses on how to control, protect, and preserve personal information [11]. Bennett [12] predicted that privacy could be used as a commodity in the information market economy, and his prediction has become true.

Thailand's Personal Data Protection act focuses on collecting, processing, disclosure, protection, and the rights of the data subjects. A violation of the PDPA could lead to a penalty of three million Thai baht [3] for the organizations. Therefore, the PDPA has raised Thai people's attention toward concerns about privacy of personal data.

In this study, we do not define privacy as any constitutional or legal concept [11]. However, this study's privacy refers to the belief and the reaction to the inside and outside stimuli. There are three categories of individuals' privacy concerns based on their level [13]. Firstly, the unconcerned privacy group. This group shows no privacy concerns at all. Secondly, those willing to disclose personal data, and thus have less privacy in exchange for the benefit they will get. Lastly, privacy absolutists refer to a group of people who have serious concerns about their privacy.

2.2 Personal health information

The GDPR considered health information as “genetic data,” which means: “Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question” [1].

Most patients voluntarily reveal their health information to receive treatment from a healthcare specialist. Examples of personal health information are demographic, allergies, symptoms, diagnoses, prescriptions, medical histories, encounter summaries, etc. Therefore, the health industry is now quickly disturbed by health information technology. That technology helps the health industry save costs, increase efficiency, improve services, and protect personal health information. One of the most famous examples of health information technology is Electronic Medical Record. The information stored in the EMR of a patient may be exposed to many individuals in the treatment processes, such as doctors, physicians, nurses, pharmacists, and technicians. Moreover, outsiders such as insurance companies and patient employers may also need to access those medical records from time to time. Therefore, the access to and storage and processing of personal health information requires the explicit adapting of inclusive policies.

2.3 Internet users’ information privacy concerns

Malhotra *et al.* [7] developed a construct for reflecting an individual’s view toward the concern of information privacy on the internet. The construct is called Internet Users’ Information Privacy Concerns (IUIPC). It contains ten-items for self-assessment questions. However, the author suggested that it should be used along with fifteen items of the CFIP (Concern for Information Privacy) scale to measure an individual's privacy concerns. Malhotra *et al.* [7] also suggested that the IUIPC should be used in the general privacy context with appropriate rewording to make the items relate to a specific context. For example, the word “online” in the questions could be eliminated so the construct can be used in the offline context [14].

Previous research applied the IUIPC to study privacy concerns in a different context. Kusyanti *et al.* [15] studied teenager's information privacy concerns on Facebook in Indonesia using the IUIPC. The result showed that the users were concerned about losing control of personal information but still had the intention of using Facebook. Sipior *et al.* [16] revalidated the method and construction of the IUIPC. The results suggested that the IUIPC construct was still applicable when applied in mobile advertising [14]. The researchers also added perceived ubiquity as an extended factor to the IUIPC. Pape *et al.* [17] re-applied the IUIPC in Japan and compared the results with results from the USA [7]. The results suggested that the IUIPC was still valid and reliable. However, trusting beliefs and risk beliefs showed some results that were contrary to those of the original IUIPC.

In the healthcare context, Angst and Agarwal [18] studied the individuals' behavioral intentions and privacy in order to digitize the medical information to the EHR. They applied the CFIP with 366 subjects. The results suggested that the appropriate message framing could increase the positive attitude toward the EHR for people in the high privacy concern group.

In conclusion, this study investigates Thai people’s behavioral intentions and concerns about sharing personal health information. We employed the constructs of IUIPC with rewording into the context of personal health information for our research model.

2.4 Research model and hypothesis

According to the literature reviewed in the previous section, the research model is shown in Figure 1. The dependent variable is the behavioral intention toward sharing health information (BI). It was predicted by Trusting Beliefs (TB) and Risk Beliefs (RB) which are independent variables. Collection (CL), Control (CR), and Awareness (AW) are independent variables used to predict the Personal Health Information Privacy Concern (PHIPC) as the dependent variable. PHIPC also acts as an independent variable to predict the Trusting Beliefs and Risk Beliefs. The definition and hypothesis of each factor are shown below.

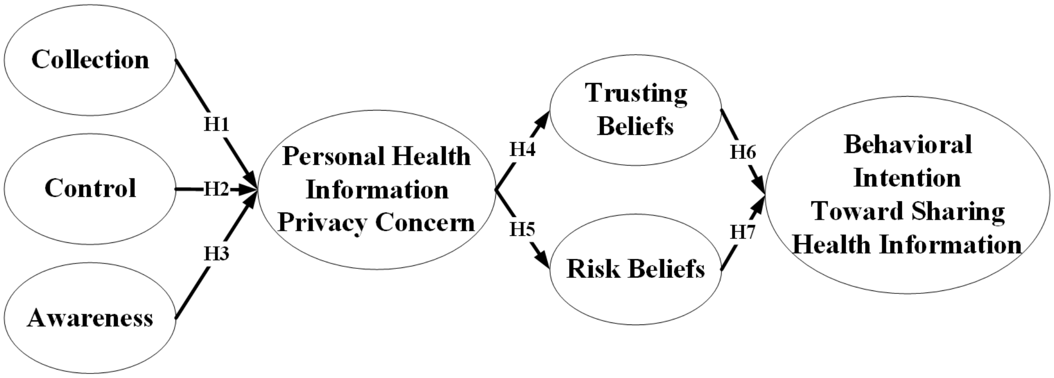
Collection
Control
Awareness
H1
H2
H3
Personal Health Information Privacy Concern
H4
H5
Trusting Beliefs
Risk Beliefs
H6
H7
Behavioral Intention Toward Sharing Health Information

Figure 1. Research model of the study

2.4.1 Collection

The collection of personal data is the beginning of information privacy concerns [7]. In this context, the collection of personal health information can be defined as "the degree to which a person is concerned about the amount of personal health data possessed by others relative to the value of benefits received" [7].

In other words, individuals would offer personal health data in return for benefits such as disease diagnosis and treatment. They may refuse to release their health data if they expect negative consequences.

H1: The collection of personal health data will positively affect personal health information privacy concerns.

2.4.2 Control

Nowadays, the GDPR requires that the data subjects have the right to control their data. The controls include obtaining consent, right of access and right of data portability, rights of rectification and erasure, right to restriction of processing and right to object, identification of data processors, and compliance of the data transfer outside the European Union [19]. The patients take high risks in revealing their health information to the health sector or third parties. Hence, control over personal health information could affect the privacy concerns of personal health information.

H2: The control of personal health data will positively affect personal health information privacy concerns.

2.4.3 Awareness

Awareness is the patient's understanding and concern for the data processors or an organization's privacy policies and practices that process their personal health information.

H3: The awareness of the data controller and data processor's privacy policy will positively affect personal health information privacy concerns.

2.4.4 Personal health information privacy concerns

Campbell [20] defined information privacy concerns as "an individual's subjective views of fairness within the context of information privacy." In this study, information privacy is the context of personal health information shared with other people or organizations.

2.4.5 Trusting and risk beliefs

Trusting beliefs are defined as "the degree to which people believe a firm is dependable in protecting consumers' personal information." Risk beliefs refer to the expectation that a high potential for loss is associated with the release of personal information to the firm [7]. Trusting and risk beliefs are the original factors in the IUIPC model. They can be used to explain how an individual reveals their personal information. Therefore, more privacy concerns may not have much effect on trusting and risk beliefs. In this context, we proposed that personal health information privacy concerns will affect trusting and risk beliefs. Moreover, trusting and risk could be the factors that affect the behavioral intention toward the release of personal health information to the healthcare sector.

H4: Personal health information privacy concerns will negatively affect trusting beliefs.
H5: Personal health information privacy concerns will positively affect risk beliefs.
H6: The trusting beliefs will positively affect behavioral intention to use the health information system.
H7: The risk beliefs will negatively affect behavioral intention to use the health information system.

2.5 Collection of data

In this study, the population of the research consists of Thai people who have experience sharing personal health information with healthcare services. Nevertheless, the total number of populations is unknown. The sample of this research was done by the accidental sampling method. Data were collected using a self-administered online questionnaire. Each of the constructs was measured with a 7-point Likert scale. The questionnaire was online for a three-week period. The URL of the questionnaire was sent to the participants via E-mail and social media services, including Facebook and Line. In the questionnaire, we explained the meaning of privacy concerns of personal health information and the control of personal health information. It was divided into two parts; the first part elicited information on demographic information and the second part was designed to test the hypothesis using the constructs from IUIPC. The collected data were recorded as a Microsoft Excel spreadsheet for data screening. The Statistical Package for Social Science (SPSS) program was used to analyze the effect between dependent and independent variables.

3. Results and Discussion

This section explains the results of the statistical analysis, including validity and reliability analysis, and multicollinearity analysis. Lastly, to test the hypotheses, four linear regression equations were used to predict the dependent variables.

3.1 Demographic variables

The total number of responses to this questionnaire was 125. Of these, 84 participants completed the questionnaire after data screening. Hence, those 84 datasets were used for empirical analysis. Table 1 shows the demographic information of the participants.

Table 1. Demographic information of the participants

Variables		Frequency	Percentage
Gender			
	Male	27	32.1
	Female	57	67.9
Total		84	100
Age			
	18-25	29	34.5
	26-33	9	10.7
	34-42	25	29.8
	More than 42	21	25
Total		84	100

3.2 Validity and reliability analysis of the constructs

The questionnaire was analyzed using the Index of Item Objectives Congruence (IOC) to confirm the validity. It was sent to 3 experts to give the points for each item. The result showed that the IOC value was more than 0.5. Therefore, the questionnaire met the criterion of validity. Furthermore, the questionnaire was also tested for reliability using Cronbach's alpha coefficient [21]. The Cronbach's alpha coefficient greater than 0.70 should be considered as a good and reliable questionnaire. The Cronbach's alpha value for each variable of the questionnaire is shown in Table 2. The Cronbach's alpha coefficient values range from 0.668-0.922 is considered highly reliable [22]. Hence, the validity and reliability requirements of the constructs were satisfied.

Table 2. The Cronbach's alpha coefficient

Factor	Number of questions	Cronbach's alpha coefficient
Trusting Beliefs	3	0.895
Risk Beliefs	3	0.794
Personal Health Information Privacy Concern	3	0.824
Collection	4	0.922
Control	3	0.668
Awareness	3	0.862

3.3 Multicollinearity analysis

The multicollinearity analysis started by examining the correlation between variables, which was done by Pearson’s product-moment correlation coefficient. It was used to assess the strength and direction of relationships between the variables. The result of Pearson’s correlation coefficient analysis from this study is shown in Table 3. It shows that some variables significantly correlated with each other. Pearson’s correlation coefficient's highest value was 0.680 at the correlation between the behavioral intention to share health information and trusting beliefs. However, Pearson’s correlation coefficient should be less than 0.8 to prevent multicollinearity. Hence, there was no issue with correlation between variables in our dataset.

Table 3. Correlation matrix of Pearson's correlation coefficient

	BI	TB	RB	CL	CR	AW	PHIPC
BI	1	.680**	.058	-.037	.130	.436**	.139
TB	.680**	1	.126	-.082	.156	.383**	.175
RB	.058	.126	1	.647**	.410**	.181	.514**
CL	-.037	-.082	.647**	1	.546**	.179	.598**
CR	.130	.156	.410**	.546**	1	.571**	.497**
AW	.436**	.383**	.181	.179	.571**	1	.340**
PHIPC	.139	.175	.514**	.598**	.497**	.340**	1

* Correlation is significant at the 0.01 level (2-tailed).

Furthermore, the constructs were analyzed to find the tolerance and Variance Inflation Factor (VIF) of variables to further confirm that there was no issue with multicollinearity. The results of those analyses are shown in Table 4. The lowest tolerance value was 0.471, and the VIF was 1.016. The highest tolerance value was 0.984, and the VIF was 2.125. The cut-off value of tolerance must not be less than 0.10, and VIF must not be more than 5 [23]. Therefore, these results confirmed that there was no multicollinearity detected between independent variables.

Table 4. Tolerance and variance inflation factor of variables

Multiple Linear Regression Model	Variables		Tolerance	Variance Inflation Factor (VIF)
	Dependent Variable	Independent Variable		
1	PHIPC	CL	0.965	1.033
		CR	0.471	2.125
		AW	0.968	1.033
2	BI	TB	0.984	1.016
		RB	0.984	1.016

3.4 Hypotheses testing results using multiple linear regression

3.4.1 Assumption testing

The collected data were tested for linearity, normality, and homoscedasticity, all of which are required for the linear regression model to be valid and reliable [24]. The normality of the data was also not violated in this study. From the graph of the normal P-P plot of standardized residuals

(Figures 2-5, left side), we can see that most of the values go along with the diagonal line in systematic order. However, model 2 (Figure 3) and model 5 (Figure 5) show some dots that depart from the diagonal line. Nevertheless, the residuals still have the pattern moving along the diagonal line. Moreover, Pallant [25] suggests that a normality assumption's violation should not be a big issue when the sample size is larger than 40. Thus, the testing of normality was satisfied.

It is usually a good way to test for linearity and homoscedasticity using the scatterplot between the regression standardized residuals and regression standardized predicted value [26]. The scatterplots of four regression models are shown in Figures 2 to 5 (right side). Homoscedasticity means that the variance of the residuals is constant. Therefore, as the predicted values increase (along the X-axis), the residuals' variation should be approximately similar. Therefore, our scatterplots suggest that the regression standardized residual values were in the range of -3.3 to 3.3, meaning no outliner, and the assumption of homoscedasticity was justified.

Field [27] suggested that the linearity issue can be investigated from the scatterplot by examining the curve in this graph. The chances are that the data have broken the assumption of linearity. This study's scatterplots show that most residuals are randomly and evenly distributed throughout the zero standard residual value line. Hence, the linearity assumption is consistent. In conclusion, this study's data met the assumptions of homoscedasticity of variance and linearity and can be used for the regression equations.

3.4.2 Regression Variate Results

A multiple linear regression equation was calculated to predict personal health information privacy concerns. Table 5 shows the results of the calculation. The regression equation is significant (F (2,81) = 28.490, $p<0.001$). The R^2 of this model is 0.413. It could predict 41 percent of the variance of PHIPC. The prediction equation for PHIPC is equal to 2.008 + 0.426 (CL) + 0.122 (CR) + 0.272 (AW) where all independent variables are measured on the 7-point Likert scale. Health information privacy concerns increased by 0.426 for one unit increase in collection and 0.272 for awareness. Collection and awareness are significant predictors of personal health information privacy concerns. The control was not significant.

There are two simple linear regression models to determine the prediction of trusting beliefs and risk beliefs. The personal health information privacy concern was used as a predictor. The results are shown in Table 6. The first model, personal health information privacy concern, is non-significant when predicting trusting beliefs. However, the regression equation is significant in the second model (F (1,82) = 29.398, p<0.001). The R^2 of this model is 0.264. It could predict 26 percent of the variance of risk beliefs. The prediction equation of risk beliefs is equal to 1.469 + 0.554 (RB). The concern of privacy in personal health information increases by 0.554 for each point of risk beliefs.

Behavioral intention toward sharing health information was predicted by the trusting beliefs and risk beliefs using a multiple linear regression model. The results of those analyses are shown in Table 7. A significant regression equation was found only with the trusting beliefs variable (F (1,81) = 70.689, p<0.001). The risk beliefs factor was found to be not significant for predicting behavioral intention toward sharing health information. The R^2 of this model was 0.463. It could predict 46 percent of the variance of behavioral intention toward sharing health information. The result predicted that behavioral intention toward sharing health information was equal to -4.117 + 0.763 (TB) + (-0.032) (RB). The behavioral intention toward sharing health information increased by 0.763 for each point of trusting beliefs.

The risk beliefs factor is also predicted by trusting beliefs. However, the trusting beliefs factor was found to be not significant for predicting risk beliefs.

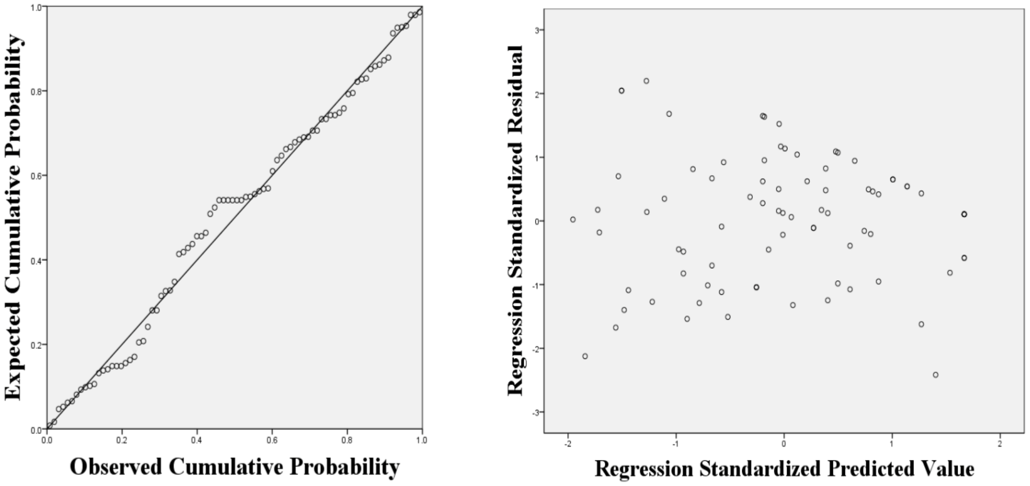

Figure 2. Model 1 normal p-p plot of regression standardized residual (left) and scatter plot (right). Dependent variable: PHIPC

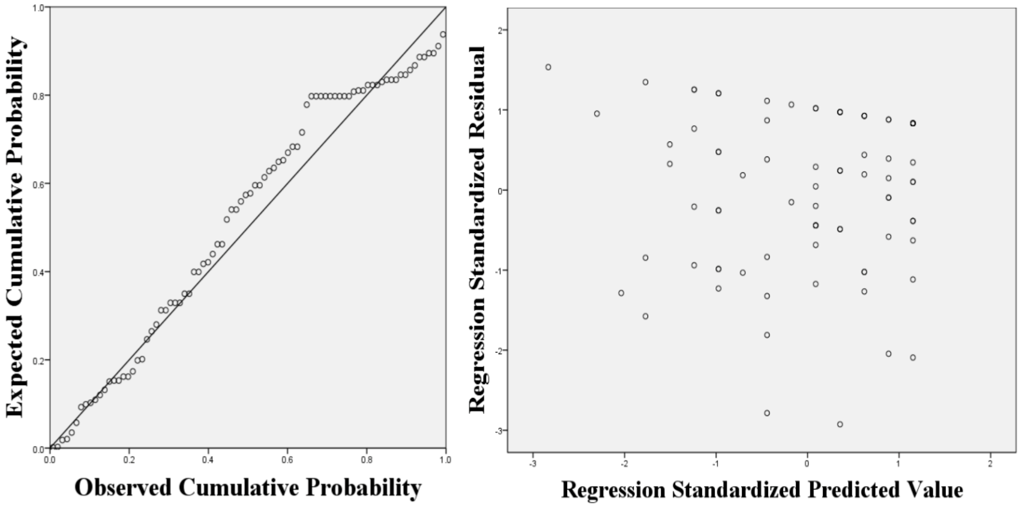

Figure 3. Model 2 normal p-p plot of regression standardized residual (left) and scatter plot (right). Dependent variable: TB

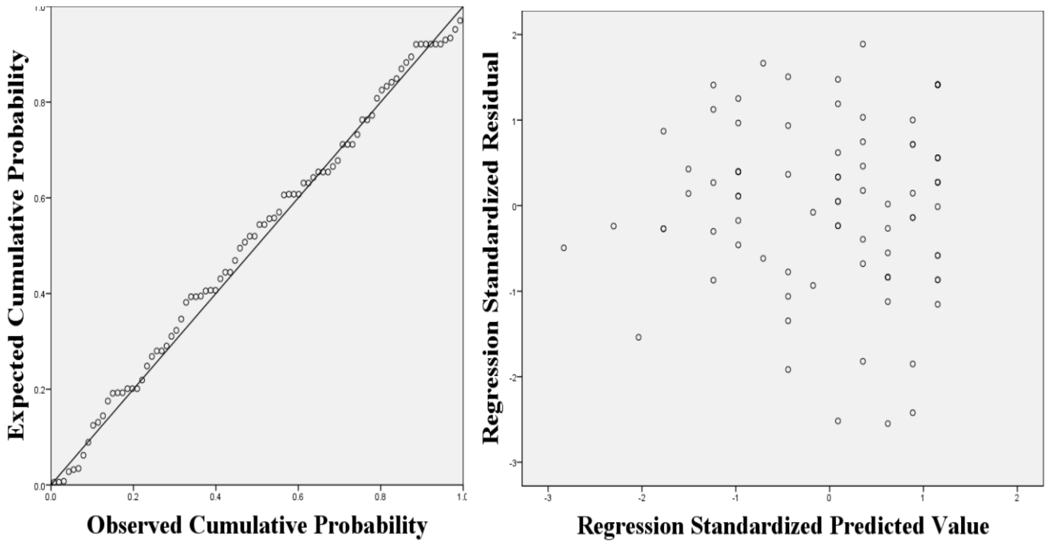

Figure 4. Model 3 normal p-p plot of regression standardized residual (left) and scatter plot (right). Dependent variable: RB

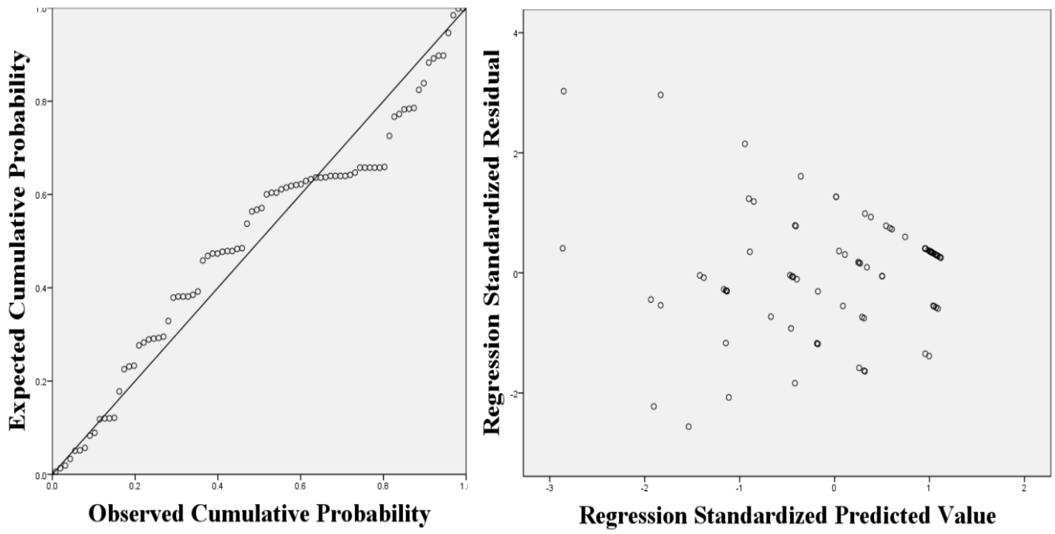

Figure 5. Model 4 normal p-p plot of regression standardized residual (left) and scatter plot (right). Dependent variable: BI

Table 5. Multiple linear regression with the collection, control, and awareness to predict personal health information privacy concerns

Independent Variables	Unstandardized Coefficients		Standardized Coefficients	t	p-value	Collinearity Statistics	
	B	**Std. Error**	**Beta**			**Tolerance**	**VIF**
(Constant)	2.008	.629		3.194	.002		
Collection	.426	.067	.555	6.409	<0.001	.968	1.033
Control	.122[c]	.983	.328	.109	.471	2.125	.471
Awareness	.272	.098	.240	2.774	<0.001	.968	1.033

*Dependent variable: Personal health information privacy concern

Table 6. Simple linear regression models with personal health information privacy concerns to predict trusting beliefs and risk beliefs

Model	Dependent Variable	Independent Variables	Unstandardized Coefficients		Standardized Coefficients	t	p-value.
			B	**Std. Error**	**Beta**		
1	Trusting Beliefs	(Constant)	4.516	.681		6.631	<0.001
		PHIPC	.192	.120	.175	1.606	.112
2	Risk Beliefs	(Constant)	1.469	.582		2.525	.014
		PHIPC	.554	.102	.514	5.421	<0.001

Dependent variable: Trusting Beliefs and Risk Beliefs

Table 7. Multiple linear regression with trusting beliefs and risk beliefs to predict behavioral intention toward sharing health information

Independent Variables	Unstandardized Coefficients		Standardized Coefficients	t	p-value	Collinearity Statistics	
	B	**Std. Error**	**Beta**			**Tolerance**	**VIF**
(Constant)	-4.117	.634		-6.495	<0.001		
Trusting Beliefs	.763	.092	.684	8.339	<0.001	.984	1.016
Risk Beliefs	-.032	.093	-.029	-.348	.729	.984	1.016

Dependent variable: Behavioral intention toward sharing health information

This study set out to assess the personal health information privacy concerns of people in Thailand. Furthermore, the second aim of this study was to investigate the factors affecting behavioral intention to share health information. The proposed research model was adapted from IUIPC [7]. We proposed and quantitatively evaluated seven hypotheses to investigate the research questions. A total of four regression analyses was used to test the hypotheses. The findings of this study are summarized as shown in Figure 6.

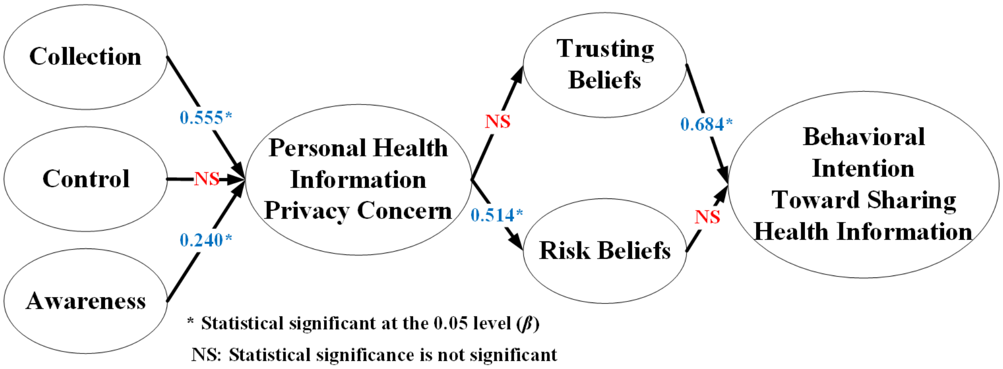
Collection
Control
Awareness
0.555*
NS
0.240*
Personal Health Information Privacy Concern
NS
0.514*
Trusting Beliefs
Risk Beliefs
0.684*
NS
Behavioral Intention Toward Sharing Health Information
* Statistical significant at the 0.05 level (β)
NS: Statistical significance is not significant

Figure 6. Results of the research model

The results showed that personal health information privacy concerns were significantly predicted by collection (β=0.555, p<0.001) and awareness (β=0.240, p<0.001). Nevertheless, the control of health information was not statistically significant when predicting personal health information privacy concerns.

Personal health information privacy concerns were significantly positively predicted by risk beliefs (β=0.514, p<0.001). On the other hand, they were negatively predicted by trusting beliefs. However, previous research suggested that personal health information privacy concerns negatively related to trusting beliefs as per our hypothesis [16]. What surprising is that trusting beliefs is the only independent variable that significantly predicts behavioral intention toward sharing health information (β=0.684, p<0.001). Therefore, the study rejected hypotheses H2, H4, and H7. On the contrary, we accepted hypotheses H1, H3, H5, and H6.

One of the more significant findings to emerge from this study is that participants will have more concerns about personal health information privacy if they have no control over the collection of personal health information. For example, if they need to provide more personal information than the doctor needs or information that seems unrelated to the disease, they will have raised their concern. These results are consistent with Malhotra *et al*. [7], Sipior *et al*. [16], and Pape *et al*. [17]. Furthermore, the awareness of how the healthcare organization processes their personal health information also affects the privacy concerns. Personal health information privacy concerns also have a positive effect on risk beliefs. If the participants are more concerned about the unclear privacy policy, they will have an increased expectation of the risks concerning their data. Surprisingly, the degree to which participants believe in protecting personal health information from the healthcare provider positively affects the behavioral intention to share health information. In accordance with the present results, previous studies have demonstrated that trusting beliefs were found to be a predictor of the user's intention to provide information [7, 16, 17], a finding that supported our results.

The PDPA will be effective in May 2021, raising awareness of Thai people's privacy concerns. The findings of this study have several important implications for supporting the PDPA. The results should facilitate compliance with the PDAPA and increase intention to share personal health information at the same time. For example, a healthcare sector should transparently make public their privacy policy that complies with Thailand's PDPA. This suggestion is based on this study's results that the trusting beliefs factor is strongly affected by the behavioral intention to share health information. Third parties that request health information, such as an insurance companies or medical laboratories, also need to demonstrate a transparent privacy policy to increase patient information collection, awareness, and trust.

4. Conclusions

In conclusion, Thai people raised privacy concerns for their personal health information based on the perception of collection of their information and awareness of the privacy policies. Thus, the healthcare industry must clarify how patients' health information will be collected, stored, and processed. Additionally, those clarifications should be available publicly to the patients. This will increase the patients' trusting beliefs, so they will be more ready to voluntarily reveal their health information. The small sample size may somewhat limit these findings. However, this study's findings will act as indicators for our planned future research into privacy concerns. An additional uncontrolled factor is the possibility that some of the participants still do not fully understand just what information privacy is about. Therefore, the interview method should be considered for future research. In addition, this research has thrown up many questions in need of further investigation. Further research should also focus on the factors that could accelerate the right level of privacy concerns in healthcare. Moreover, privacy concerns in other industries should be investigated.

5. Acknowledgments

The authors would like to express their gratitude to Univ.-Prof. Dipl.-Ing. Dr. Gerald Quirchmayr at the University of Vienna for his valuable recommendations on the research topic.

References

[1] European Union, 2019. *Complete Guide to GDPR Compliance*. [online] Available at: https://gdpr.eu/

[2] EUR-Lex, 2019. *Regulation (EU) 2016/679 of the European Parliament and of the Council.* [online] Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/

[3] Thai Government, 2019. *Personal Data Protection Act*. [online] Available at: https://drive.google.com/open?id=1MzGNi3kdDPA0E52n8bDybeuDNklM8xJe.

[4] HIQA, 2017. *Privacy Impact Assessment Toolkit for Health and Social Care.* [e-book] Dublin: Health Information and Quality Authority.

[5] WP29, 2016. *Article 29 - Data Protection Working Party*. [Online] Available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

[6] Theera-ampornpunt, N., 2009. *Medical Informatics: A Look from USA to Thailand.* [Online]. Available at: https://scholar.google.co.th/scholar?hl=th&as_sdt=0%2C5&q=Medical+Informatics%E2%80%AF%3A+A+Look+from+USA+to+Thailand&btnG=

[7] Malhotra, N.K., Kim, S.S. and Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.

[8] Altman, I., 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3), 66-84.

[9] Solove, D.J., 2002. Conceptualizing privacy. *California Law Review*, 90(4), 1087-1155.

[10] Margulis, S.T., 1977. Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5-21.

[11] Margulis, S.T., 2003. Privacy as a social issue and behavioral concept. *Journal of Social Issues*, 59(2), 243-261.

[12] Bennett, C.J., 1995. *The Political Economy of Privacy: A Review of the Literature.* University of Victoria, Department of Political Science, Victoria.

[13] Westin, A.F., 2003. Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453.

[14] Okazaki, S., Molina, F.J. and Hirose, M., 2012. Mobile advertising avoidance: exploring the role of ubiquity. *Electronic Markets*, 22(3), 169-183.

[15] Kusyanti, A., Puspitasari, D.R., Catherina, H.P.A. and Sari, Y.A.L., 2017. Information privacy concerns on teens as Facebook users in Indonesia. *Procedia Computer Science*, 124, 632-638.

[16] Sipior, J.C., Ward, B.T. and Connolly, R., 2013. Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management*. 26(6), 661-678.

[17] Pape, S., Ivan, A., Harborth, D., Nakamura, T., Kiyomoto, S., Takasaki, H. and Rannenberg, K., 2020. Re-evaluating internet users' information privacy concerns: the case in Japan. *AIS Transactions on Replication Research*, 6(18), 1-18.

[18] Angst, C.M. and Agarwal, R., 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339-370.

[19] Commission Nationale de l'Informatique et des Libertés, 2018. *Privacy Impact Assessment (PIA) Methodology*. [online] Available at: https://www.cnil.fr/en/privacy-impact-assessment-pia

[20] Campbell, A.J., 1997. Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Direct Marketing*, 11(3), 44-57.

[21] Santos, J.R.A., 1999. Cronbach's alpha: A tool for assessing the reliability of scales. *Journal of extension*, 37(2), 1-5.

[22] Nunnally, J.C., 1994. *Psychometric theory 3E*. New Delhi: Tata McGraw-hill Education.

[23] Hair, J.F., Anderson, R.E., Tatham, R.L. and Black, W.C., 1998. *Multivariate Data Analysis*. 5th ed. Upper Saddle River: Prentice Hall.

[24] Tabachnick, B.G. and Fidell, L.S., 2007. *Using Multivariate Statistics*. Boston: Pearson.

[25] Pallant, J., 2020. *SPSS Survival Manual: A Step-by-Step Guide to Data Analysis using IBM SPSS*. 7th ed. Milton: Routledge.

[26] Allen, P.J. and Bennett, K., 2007. *SPSS for the Health and Behavioural Sciences*. South Melbourne: Thomson Learning.

[27] Field, A., 2009. Discovering Statistics Using SPSS. 3rd ed. London: SAGE Publications Ltd.