ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse155942020.pdf
https://doi.org/10.30534/ijatcse/2020/155942020

User Privacy Protection Behavior and Information Sharing in Mobile Health Application

Kong Jia Hui[1], Syarulnaziah Anawar[2], Nur Fadzilah Othman[3], Zakiah Ayop[4] Erman Hamid[5]
[1]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malaysia, jhkong1230@gmail.com
[2]Center for Advanced Computing Technology , Fakulti Teknologi Maklumat dan Komunikasi , Universiti Teknikal Malaysia Melaka, Malaysia, syarulnaziah@utem.edu.my
[3]Center for Advanced Computing Technology , Fakulti Teknologi Maklumat dan Komunikasi , Universiti Teknikal Malaysia Melaka, Malaysia, fadzilah.othman@utem.edu.my
[4]Center for Advanced Computing Technology , Fakulti Teknologi Maklumat dan Komunikasi , Universiti Teknikal Malaysia Melaka, Malaysia, zakiah@utem.edu.my
[5]Center for Advanced Computing Technology , Fakulti Teknologi Maklumat dan Komunikasi , Universiti Teknikal Malaysia Melaka, Malaysia, erman@utem.edu.my

ABSTRACT

The use of mobile health applications provides a convenient platform to the healthcare sector for conducting self-health monitoring, efficient consultation, health goals achievement, customer's information data storage, and others. There are growing concerns about privacy in mobile health platforms, particularly when highly sensitive health data is involved. Sharing personal information in mobile health applications does bring risks to the users, which might lead to the leaking of confidential information, and misuse of information. Due to this, protecting one's information has become essential when using the platform. Therefore, this paper aims to investigate the influence of users' privacy protection behavior in shaping users' willingness in sharing information in mobile health applications. This paper adopted a quantitative methodology where data from a survey (N=200) of mobile health application users is analyzed. This study proposed a model that offers understandings on which users' privacy protection factors could stimulate users to share their information in a mobile health platform. Based on the results, this study concluded that response efficacy has the highest influence on information sharing, followed by vulnerability, self-efficacy, and perceived susceptibility-medical info. The proposed model may benefit other researchers attempting to understand user standpoint's on data privacy compliance in mobile health application and increase user awareness in the research area

Key words: Health Belief Model, Privacy, Mobile Health, Protection Motivation Theory.

1. INTRODUCTION

In the healthcare sector, the expansion of using mobile devices has provided this opportunity for the creation and release of mobile health applications. Currently, over 97,000 mobile health applications (termed as mHealth apps hereafter) are offered in the health and fitness category of the Google Play and Apple app stores [1]. Mobile health as known as mHealth refers to the practice related to health care and medicine using mobile devices; for instance, smartphones, tablets, wearable devices, and others. There is considerable interest in the mHealth concept, where the term is usually used to describe the use of mobile technologies for the wellness support and delivery of health care [2].

In recent years, the role of mHealth apps in improving user accessibility to health information, clinical care, and resources has grown rapidly [3]. The use of mHealth apps provides a convenient platform to healthcare providers and consumers for conducting professional communication, efficient consultation, health goals achievement, customer's information data storage, and others. Such platforms include health text messaging, remote monitoring, and portable sensor devices. mHealth apps can be used to monitor various health information such as activities (Fitbit [4]), sleep (Tuck [5]), emotions (Affectiva[6]), vital signs like blood pressure (Withings [7]) or fetal conditions (Monica AN24 [8]).

One of the main challenges that obstruct the development of mHealth is the need for better provision of healthcare, where the technical issues cause its poor integration with the present health systems [9]. On top of these, issues like privacy, security, and trust will affect the deployment of mHealth [10]. Some mHealth apps provide health care services based on the data collected from users. Due to this, user attitudes towards privacy in information sharing need to be observed. The observation could be done through continuous data collection over a long period [11] using daily location tracking, daily medicine consuming reminders, and others. These require appropriate data management [12]. Inappropriate data management will make people reluctant to

share their personal information, as they are aware of the likelihood of their data being misused or exploited.

This study seeks to answer the following research questions: What are the privacy protection factors for information sharing in Mobile Health application? Guided by a theoretical foundation in Protection Motivation Theory [13] and Health Belief Model [14], our research model attempts to investigate the privacy protection factors to be considered as part of the information sharing in the mobile health application.

This paper is organized as follows: The first part of the paper reviews the information sharing concept and presents related work on privacy protection in mHealth application. Next, theoretical framework development is proposed by extending the Protection Motivation Theory (PMT) and Health Belief Model (HBM) in a mobile health setting. Subsequently, this paper provides the details on research methodology and presents the findings of data analyses. Finally, the findings are discussed and concluded in this paper.

2.LITERATURE REVIEW

This section provides a fundamental understanding of privacy and information sharing in mobile health applications.

2.1 Privacy Protection in mHealth apps

In the context of Information Systems, privacy is defined as "an individual's tendency to be concerned about overall information privacy" [15]. Privacy protection is directly related to basic human needs and is a common issue among users of the Internet [16]. Privacy protection is important in mHealth apps to protect confidential information, to prevent unauthorized access [17], and to prevent misuse of medical record [18]. User's intention to adopt certain privacy protection indicates their attitude towards protective strategies offered by mHealth apps provider, where the action might be influenced by previous experiences, and self-ability to protect their private information.

The use of mHealth apps enables the sharing of information among patients, apps users, healthcare entities. The sharing of information enables more than one party to communicate and access health-related information electronically. Previous studies indicated that socio-demographic characteristics and the type of health information shared in the platform can affect information sharing [19]. The socio-demographic characteristic that influences information sharing may include the familiarity use with mHealth apps, self-efficacy, and trust in apps [19-20].

It is believed that willingness on sharing health information may vary on the type of health information required by particular mHealth apps. The types of health-related information can be presented in three main categories namely personal information, medical information, and lifestyle information [19] [21]. Personal information includes age, weight, height, email, and phone number. With regard to medical information, the information can be body test results, genetic information, and health history, mental and sexual information. Finally, lifestyle information may include sleep, heart rate, calorie intake, walking distance, and so on.

2.2 Privacy Challenges in Information Sharing

Sharing health information online does bring challenges to the users, which might lead to a serious condition such as the leaking of confidential information, or misuse of information through network attack. In the healthcare sector, privacy issues do not only concern the patients, but also the doctors, medical practitioners, and service providers [21]. Moreover, in the era of big data, challenges on data privacy are not focusing on individual health information. Big data relies on the analysis and research of people's data, and the targeted prediction of population's state and behavior [22].

Consequently, the rapid exchange of health information has become common activities in mHealth apps. Inadequate data privacy management may cause a distrust of the mHealth technologies, and negatively impact the success of the system. The rising number of mHealth apps could pose a serious privacy concern, as it causes unfamiliarity with the app's environment [23] as users are usually uninformed of how their data are managed and used [24]. User's concern regarding their right may influence their decision on sharing health information on the platform. [18] states that mHealth users are mostly concerned with data misused by third parties and whether they might not gain the benefits from information sharing.

3.THEORETICAL FRAMEWORK

This section presents the adaptation of the Protection Motivation Theory (PMT) and Health Belief Model (HBM) into privacy protection constructs in mobile health. Additionally, this section provides the formation of hypotheses and the operational definition for the proposed theoretical framework.

3.1 Theoretical Framework

Protection Motivation Theory (PMT) [25-26] provides conceptual clarity to understand an individual's fear of appeal and behavioral change towards certain conditions or environments. In healthcare fields, PMT is used mainly as a model to explain the decision making of people and actions taken in certain conditions related to health. PMT mainly consists of four constructs, which are Perceived Vulnerability (PV), Perceived Severity (PS), Response Efficacy (RE), and Self-Efficacy (SE). All of these variables are grouped into two categories. In the PMT, perceived severity and perceived vulnerability constructs are categorized into threat appraisal categories, while response

efficacy and self-efficacy constructs are categorized under the coping appraisal category. The threat appraisal category emphasizes on the ability of a user to avoid security risks and incidents due to their perception on threat vulnerability and severity. On the other hand, coping appraisal emphasizes the ability of a user to avoid security risks and incidents due to their belief in successfully implementing the recommended security practice.

Alternatively, the Health Belief Model (HBM) is a social cognitive model for the health sector and is used to explain and predict individual health behavior [14]. HBM includes several constructs, which are perceived susceptibility, perceived severity, perceived threat, perceived benefit, perceived barriers, self-efficacy, and cue to action. HBM is useful in deriving information that may prompt health behavior interventions. However, using the model alone to enlighten decision making in the context of data privacy is insufficient, as the model could not explain how such interventions might best be structured.

The proposed theoretical framework integrates the previously identified constructs in both PMT and HBM theories. The theories are adapted based on their application to screening behavior, and the prediction they offer based on some of the research done in the health area. The combination of theories holds promise to further understand user behavior while using mHealth apps as it is crucial to consider association and dependency between constructs [27]. The integration of both theories is important due to the limitation of HBM, in that it is a cognitive-based model and does not consider the emotional component of behavior.

Previously, [27] had experimented in combining HBM and PMT to predict screening mammography behavior by adding fear variable to the HBM. The study found an association between the HBM constructs and the fear variable. Fear was significantly predicted by perceived threat, benefits, and self-efficacy, which can be conceptualized as a predictive state that protects one from danger [28]. Therefore, it can be interpreted that fear derived from PMT does provide stimulation on response efficacy from HBM in taking precautionary action. The results corroborate with the Protection Motivation Theory.

This paper proposes the theoretical framework as shown in Figure 1. Essentially, this study re-examines the constructs as privacy protection factors concerning information sharing in mHealth setting. This study only extracts perceived susceptibility and cues to action from HBM into the theoretical framework as a detailed examination of HBM indicates that other constructs in HBM have been used in similar ways to PMT. Hence, there are six constructs are employed in the study which are perceived susceptibility, perceived vulnerability, perceived severity, self-efficacy, response efficacy, and cues to action.

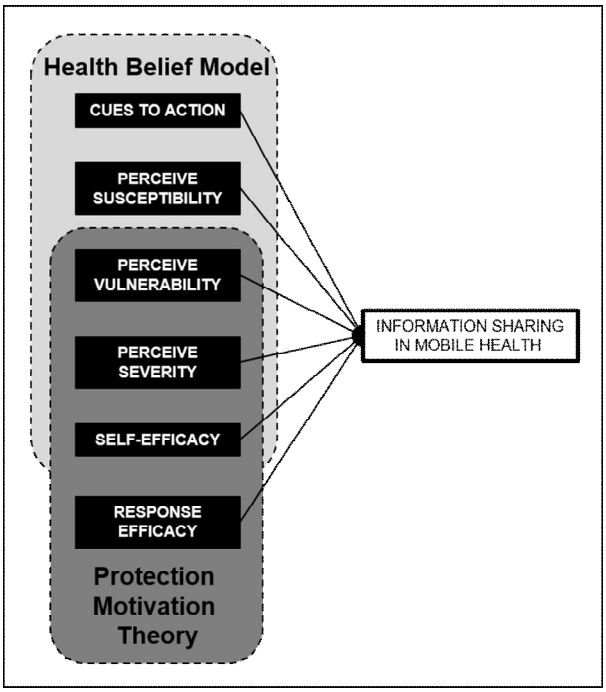

Figure 1: Proposed Privacy Protection Framework for mHealth

3.2 Operational Definition

Table 1 shows the proposed operational definitions for the variables used in this study.

Table 1: Operation Definitions of Variables

Variables	Operational Definition
Information Sharing	A person's unwillingness for sharing health information.
Perceived Susceptibility	A person's opinion on the degree of sensitivity of information shared in mHealth apps.
Perceived Vulnerability	A person's concern or judgment of the likelihood of threat when information is shared in mHealth apps.
Perceived Severity	Measurement of one's perceived risk which could lead to a serious condition when sharing information in mHealth apps.
Self-efficacy	A person's judgment on his/her ability to share information in mHealth apps.
Response Efficacy	The degree to which an individual believes the information shared is for beneficial purposes that protects them from a threat.

3.3 Variable Identification and Formation of Hypotheses

Perceived Susceptibility. Different individual has different opinions on defining how sensitive a piece of particular health information is. People considered health-related information as private matters, which do not warrant sharing with others [1]. In [1], the sensitivity of health information is discussed, in health information has higher sensitivity than other types of personal information. However, the perceived sensitivity of health information differs from one individual to another [21]. The study's finding is consistent with [29] findings which showed that users will feel that they are more

susceptible to privacy risk when the sensitivity of the information is higher,. Additionally, it is found that perceived susceptibility of health information reduces the willingness of an individual to disclose sensitive information [30] and influences an individual's privacy concern on health information [31]. Therefore, the following hypothesis is proposed:

H1: *Perceived susceptibility has an association with unwillingness in information sharing.*

Perceived Vulnerability. [3] states that the higher the perceived vulnerability, the more likely a user's privacy is exposed to the risk of data exploitation. This could lead to a serious condition where user information could be used for marketing purposes or criminals to harm the user. [23] shows the concern of how the information might be misused and exploited by a third party, such as advertisers or health insurance companies. In another study [1], the concern is more prominent with observed data in mHealth apps such as routine running, in which users believe that personal information routes could put them in danger. The joint effects of perceived vulnerability and perceived severity provide the force to take preventive action which leads to the willingness to share information [32]. Therefore, the following hypotheses are proposed:

H2a: *Perceived vulnerability has an association with perceived severity.*

H2b: *Perceived vulnerability has an association with unwillingness in information sharing.*

Perceived Severity. An individual who perceived higher severity is going to have higher information privacy concerns [33]. If a user believed that information disclosure to a specific party like a service provider or medical practitioner will result in negative outcomes, the user will express higher privacy concerns on health information and may be less willing to share the information [21]. Therefore, the following hypotheses are proposed:

H3: *Perceived severity has an association with unwillingness in information sharing.*

Self-efficacy. [34] regards self-efficacy as an individual's judgment of his or her capabilities to perform tasks. In other words, self-efficacy determines strong predictive ability [35] towards personal behavior through motivational, cognitive, social influence, and effective intervening processes. Individuals with high self-efficacy have more confidence in their ability to manage their private information as well as have fewer privacy concerns when sharing information [23]. On the other hand, lower self-efficacy individuals' are more likely to value their privacy because they feel incompetent in deciding when and where they should share their information.

H4: *Self-efficacy has an association with unwillingness in information sharing.*

Response Efficacy. [35] argues that social influence has slightly more of an effect on behavioral intent. Response efficacy evaluates how effective an adaptive response reduces or eliminates a threat. [36] showed that response efficacy is likely to play a key role in lowering the risk of information disclosure. Individuals who perceived more privacy protection from the system provider have less system-specific privacy concerns and are more willing to share health information [37]. Additionally, individuals will feel that they can mitigate threats if they apply the recommended behavior by the service provider, thus limiting the amount of information shared in the platform.

H5: *Response efficacy has an association with unwillingness in information sharing.*

Cues to Action. Cues to action is an action taken to trigger awareness regarding privacy when sharing personal health information in mHealth apps. Some of the possible action that users can take in mHealth apps is to enable nudges and reminders in the apps. This will reduce possible gaps between user concerns on privacy and the actual sharing actions by the users [38]. A positive intention towards a behavior can provide cues to perform the behavior and preventing mistakes to happen [35].

H6: *Cues to action has an association with unwillingness in information sharing.*

4.METHODOLOGY

This section provides the details on quantitative methodology adopted in the study.

4.1 Instrument Design

This study used a structured questionnaire for data collection. The questionnaire is divided into three parts, namely part A, B, and C. In part A, a participant is required to provide personal basic information. Part B is to indicate the basic knowledge of participants in Mobile Health. Part C includes questions to evaluate the six constructs in the theoretical framework. Most of the items in part C are adapted from previous studies such as [41], [23], [36], and are then modified to fit the context of the present study.

The question used a 6-point Likert scale that measures statements of the agreement for each item. However, for the perceived susceptibility variable, the Likert scale measures degree of information sensitivity that ranged from not sensitive (1) to extremely sensitive (6). The final questionnaire consists of 37 items to investigate basic knowledge of mobile health application, and the variables listed in the framework. Items used to measure an individual's unwillingness in information sharing were developed by adapting items from existing literature.

Before actual data collection, the questionnaire is validated through different analyses like content validation, pilot testing, and construct validation. Content validation is done by three experts, with a minimum experience of 10 years

from the information security and health informatics field. 50 participant's responses are selected for the pilot test. As the targeted scale is small, the questionnaire is distributed in paper form. The pilot test data collection is approximately 3 weeks. Data collected from participants will undergo further analysis like item analysis and factor analysis. During the validation process, modification and elimination of items are made. Once all these processes complete, data collection is carried out on a larger scale.

4.2 Data Collection

The sampling method used is a proportional quota sampling. In this study, the selection of participants is based on gender, which consists of an equal number on both males and females. The biggest advantage of using the quota-sampling method is that data collected based on gender are well balanced, therefore, there will be no bias case on one side, which could lead to inaccuracy of analysis result.

200 participants are set as the survey respondents. A ratio of 1:1 is targeted which data collected will be balance based on gender. The sample size is adapted from a previous study [42] who stated that 200-500 of responses are considered as a good size sample for further analysis such as regression analysis or covariance analysis. The data collection took around 2 months to reach the number of sample targets. All data collected is entered into an IBM SPSS for further analysis. As there are no missing data, data screening is not required.

5.RESULTS

This section presents the result of data analysis involved in this study namely item analysis, factor analysis, correlation analysis, and regression analysis.

5.1 Item Analysis

Item analysis is carried out after the collection of pilot test data. Item analysis is also known as a reliability test that analyzes the reliability of items based on Cronbach's alpha. A minimum of Cronbach's alpha value 0.7 is required so that the correlation of items is strong. The results of the item analysis are shown in Table 2.

Table 2: Results of Item Analysis

Variables	Before Revision		After Revision	
	Cronbach Alpha	No. of Items	Cronbach Alpha	No. of Items
Perceived Susceptibility	0.825	11	0.825	11
Perceived Vulnerability	0.858	4	0.858	4
Perceived Severity	0.819	4	0.819	4
Self-Efficacy	0.575	6	0.706	4
Response Efficacy	0.670	4	0.868	3
Information Sharing	0.707	4	0.707	4

All items are analyzed to test its reliability based on different variables. The total number of items is from six variables is 33. Results of item analysis show that there are four variables with good Cronbach's alpha value, which exceed 0.7. The variables are perceived susceptibility, perceived vulnerability, perceived severity, and information sharing which stated 0.825, 0.858, 0.819, and 0.707 respectively. The other variables did not meet the minimum required value of 0.7. Therefore, items in self-efficacy and response efficacy variables were revised again for further elimination.

5.2 Factor Analysis

Principal component analysis to reduce the number of variables into smaller numbers of components, which still contain complete information in the samples. In this study, Varimax rotation is used as it is an orthogonal rotation method that has high potential to minimize the number of variables that have high loadings on each factor. The results of the principal component analysis are shown in Table 3.

Table 3: Results of Principal Component Analysis

Item Code	1	2	3	4	5
Perceived Vulnerability (PV)					
PV01	0.805				
PV03	0.823				
PV06	0.800				
PS01	0.787				
PS02	0.827				
PS04	0.669				
PS05	0.838				
Perceived Susceptibility -Medical info (SSM)					
SS04		0.689			
SS05		0.724			
SS08		0.814			
SS09		0.721			
SS11		0.756			
Self-efficacy (SE)					
SE01			0.576		
SE03			0.849		
SE05			0.832		
SE06			0.567		
Response Efficacy (RE)					
RE02				0.847	
RE03				0.933	
RE04				0.874	
Perceived Susceptibility - Personal info (SSP)					
SS01					0.731
SS02					0.631
SS03					0.732

Total amount of variance	8.888	3.090	2.493	1.765	1.414
Total % of variance	34.18	11.88	9.590	6.789	5.437

There are a total of 26 items in independent variables. All items were grouped based on their highest factor loadings. Based on the results, five factors are extracted based on the grouped items. The extracted factors structure explained 67.88%, of the variance, which is sufficient for social science research. A minimum of three items should be loaded in each factor; otherwise, the factor will be eliminated. In this case, factor 6 is eliminated as it only consists of two items which are SS07 and SS13. The factor loading for both SS07 and SS13 is 0.804 and 0.784 respectively. Since it is insufficient of items in factor 6, factor 6 is not used even the factor loading of its items is high. Additionally, both SS06 and PV02 are eliminated due to low commonalities.

The remaining five factors are renamed and will be explained accordingly based on its items grouping, factor loadings, and others. Two factors are dropped from this study: Perceived Severity and Cue to Action. The final factors extracted from the analysis are Perceive Vulnerability, Perceived Susceptibility-Medical Info, Perceived Susceptibility-Personal Info, Self-Efficacy, and Response Efficacy. Finally, the updated total number of items in the questionnaire is 22.

5.3 Correlation Analysis

In this study, the Spearman correlation method is used because the data collected indicated a non-normal distribution after performing Kolmogorov-Smirnov. Based on the two-tailed significance values of the correlation between variables, the significance level used in this study is 0.01. This study only considers a p-value of 0.01 as the results show that most associations were weak and moderate. The result of the correlation analysis is presented in Table 4. The correlation coefficient was determined between the independent and dependent variables. From the results, it can be seen that all variables are significantly associated with information sharing in mobile health. Therefore, H1a, H1b, H2b, H4, and H5 are accepted.

Table 4: Results of Correlation Analysis

	SSP	SSM	PV	SE	RE	IS
SSP	1.000					
SSM	0.714**	1.000				
PV	0.676**	0.717**	1.000			
SE	0.137	0.207**	0.260**	1.000		
RE	0.256**	0.122	0.197**	0.104	1.000	
IS	0.274**	0.410**	0.404**	0.211**	-0.311**	1.000

5.4 Structural Equation Modeling

The variables were then evaluated in Structural Equation Modeling (SEM) to establish a valid model. This study used Amos to analyze several goodness-of-fit indices. Some of the values that were taken into account are Goodness of Fit Indices (GFI), Tucker- Lewis Index (TLI), Comparative Fit Index (CFI), and Root Mean Square (RMR). This study uses the acceptable model fit indices as seen in Table 5 based on the guideline in [40-41].

Table 5: Results of Correlation Analysis

Model	Accepted Value	Framework Value
x^2/df	<=5	2.539
GFI	>0.95	0.998
CFI	>0.95	0.995
TLI	>0.95	0.990
RMR	<0.05	0.013

The evaluated model shown in Table 6 reveals adequate goodness of fit, in which Perceive Vulnerability, Perceived Susceptibility-Medical Info, and Self-Efficacy variables are positively influenced information sharing in mobile health application. On the other hand, it can be seen that Response Efficacy negatively influence information sharing.

Table 6 presents the results of the regression weight acquired from the SEM analysis. In the table, Estimate is the regression value between the variables, S.E w stands for Standard Error and C.R is the Critical Ratio. Three asterisk symbols in the P column indicate that the p-value is 0.001, which means the association between the variables is highly significant.

Table 6: Results of Regression Weight

	Estimate	S.E.	C.R.	P
RE ← SE	.243	.113	2.144	.032
SSM ← SE	.459	.125	3.687	***
PT ← RE	.175	.059	2.994	.003
PT ← SSM	.695	.052	13.332	***
IS ← SSM	.129	.058	2.212	.027
IS ← SE	.192	.079	2.429	.015
IS ← PT	.235	.057	4.146	***
IS ← RE	-.341	.048	-7.053	***

From the results, it can be seen that the majority of p-value referring to the association between two variables is statistically significant under a significant value of 0.01. However, there are few associations between two variables are not statistically significant. From the estimates obtained, the equation obtained from multiple regression analysis is verified, whereby all the estimates are the same as the values obtained:

Information Sharing = 3.252 – 0.341RE + 0.235PV + 0.192SE + 0.129SSM

Where:

IS= Information Sharing
RE= Response Efficacy
PV= Perceived Vulnerability
SSM= Perceived Susceptibility (Medical)
SE= Self-efficacy

From the regression equation, the highest contribution to information sharing is response efficacy which has a value of -0.341, followed by 0.235 from perceived vulnerability, 0.192 from self-efficacy, and lastly 0.129 from perceived susceptibility-medical information. Therefore, the proposed model is considered as a good model as the values of fit indices presented represent a good model fit.

6. DISCUSSION

During factor analysis, items from perceived vulnerability and perceived severity are grouped as one factor. It was found that the items from both variables measure the same thing. The group is named as perceived vulnerability as the items from perceived vulnerability variables dominate the factor. In addition, the factor analysis formed two new factors under perceived susceptibility variable namely perceived susceptibility-medical info and perceived susceptibility- personal info.

Further elimination of perceived susceptibility- personal info is done during regression analysis due to its insignificant effect on information sharing. Based on the regression output, it can be seen that response efficacy has the highest effect on information sharing in mobile health, followed by perceived vulnerability, self-efficacy, and perceived susceptibility-medical info.

Based on the proposed model, it could be seen that the response efficacy inversely influences the unwillingness of information sharing in mobile health. A person with low response efficacy tends to share more information in the mHealth application. The inverse influence of response efficacy variable is not surprising, as users usually consider the privacy condition stated by the system provider when deciding to share their health information. The level of response efficacy typically reflects users' belief concerning service provider's ability in protecting user's information, or it's misused, such as disclosure to third parties or secondary use without the consent of the concerned users [41]. When users know that their health information is in proper use, they will be more willing to share their information rather than to care for information privacy [44].

Furthermore, self-efficacy is positively associated with several independent variables namely perceived susceptibility-medical info and response efficacy. This finding corroborates the ideas of [37], who suggested that the ability to think, feel, and motivate might cause higher awareness of privacy, which eventually influences user behavioral intent [37]. Therefore, when a user has a higher level of self-efficacy, they will have more confident in privacy knowledge [46] and tends to restrict information sharing in Mobile Health application.

Perceived susceptibility-medical info is positively associated with variable information sharing. It is indicated that a higher level of perceived susceptibility in medical information causes a higher level of the unwillingness of information sharing. As highlighted earlier, users are less willing to share health-related information as it is perceived to be of higher sensitivity compare to other types of information [19].

7. CONCLUSION

This paper set out to determine the privacy protection factors to be considered as part of information sharing in the mHealth application. The factors are derived from the Protection Motivation Theory and Health Belief Model. This study has shown that response efficacy has the highest influence on information sharing, followed by vulnerability, self-efficacy, and perceived susceptibility-medical info. In addition, this study has found that users believe that they are more susceptible to security threats if they disclose health-related information compare to personal information. This study contributes to the new knowledge and awareness of privacy in mobile health applications.

There are some limitations found during the progress of this study. Data sampling only focuses on gender criteria and does not fully represent the population in all aspects. Therefore, future work should seek to expand the influence of different demographic factors towards information sharing in mobile health.

ACKNOWLEDGEMENT

The authors would like to thank our research instrument reviewers; Mohd Fairuz Iskandar Othman, Zuraida Abal Abas, and Mohd Zaki Mas'ud for their insightful comments. A high appreciation to Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) for supporting the work done in this paper.

REFERENCES

1. W. Peng, S. Kanthawala, S. Yuan, and S. A. Hussain. **A qualitative study of user perceptions of mobile health apps**. *BMC public health*, Vol. 16 no. 1, pp.1-11, 2016. https://doi.org/10.1186/s12889-016-3808-0
2. S. R. Steinhubl, E. D. Muse, and E. J. Topol. **Can mobile health technologies transform health care?**, *Jama*, Vol. 310, no. 22, pp. 2395-2396, 2013.
3. A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz. **Understanding sharing preferences and behavior for mHealth devices**, in *Proc. 2012 ACM workshop on Privacy in the electronic society*, 2012, pp. 117-128.

4. Fitbit.(n.d). http://www.fitbit.com, July 2020.
5. Tuck. .(n.d). http://www.tuck.com, July 2020.
6. Affectiva.(n.d). http://www.affectiva.com. July 2020.
7. Withings blood pressure cuff. .(n.d). http://www.withings .com, July 2020.
8. Monica AN24. .(n.d). http://www.monicahealthcare.com, July 2020.
9. S. Anawar, W. A. W. Adnan, and R. Ahmad. **A design guideline for non-monetary incentive mechanics in mobile health participatory sensing system**. *International Journal of Applied Engineering Research*, vol. 12, no. 21, pp. 11039-11049, 2017.
10. P. Quinn, A. K. Habbig, E. Mantovani, and P. De Hert. **The data protection and medical device frameworks—obstacles to the deployment of mHealth across Europe**, *European Journal of Health Law*, vol. 20 no. 2, pp.185-204, 2013. https://doi.org/10.1163/15718093-12341267
11. M. S. Jeffree, F. Ahmedy , R. Avoi, M. Y. Ibrahim, S. S. Syed Abdul Rahim, F. Hayati , J. L. Loo, and N. Mohd Tuah. **Integrating Digital Health for Healthcare Transformation: Conceptual Model of Smart Healthcare for northern Borneo**, *International Journal of Advanced Trends in Computer Science and Engineerings*, vol. 9, no. 1, pp. 110-115, 2020. https://doi.org/10.30534/ijatcse/2020/17912020
12. S. Anawar, Y. W. Hong, E. Hamid, and Z. Ayop. **Content Analysis of Privacy Management Features in Geosocial Networking Application**, *International Journal Of Advanced Computer Science And Applications*, vol. 9, no. 11, pp. 476-484, 2018.
13. Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory.
14. R. W. Rogers, and S. Prentice-Dunn. **Protection motivation theory**, in *Handbook of health behavior research 1: Personal and social determinants*, D. S. Gochman, Ed., Plenum Press, 1997, pp. 113–132.
15. N. K. Janz, and M. H. Becker. **The health belief model: A decade later**, *Health Education Quarterly*, vol. 11, no. 1, pp. 1-47, 1984.
16. Y. Li. **Empirical studies on online information privacy concerns: literature review and an integrative framework**, *Communications of the Association for Information Systems*, vol. 28, no. 1, pp. 453-496, 2011.
17. K. S. JN. Prasad, and C.Srinivas. **Security and Privacy in Cloud Computing To Guarantee Simultaneous Localization of Data Errors,** *International Journal of Advanced Trends in Computer Science and Engineerings*, vol. 4, no. 1, pp. 19-27, 2015.
18. M. Z. Yao, and D. G. Linz. **Predicting self-protection of online privacy**, *CyberPsychology & Behavior*, vol. 11, no. 5, pp. 615-617, 2008. https://doi.org/10.1089/cpb.2007.0208
19. A. M. Yunus, and A. Mohammad. **A Proposed framework based electronic medical records (ERM) for implementation of technology acceptance in healthcare service**, *International Journal of Academic Research in Business and Social Sciences*, vol. 7, no. 9, pp. 96-115, 2017.
20. K. J. Serrano, M. Yu, W. T. Riley, V. Patel, P. Hughes, K. Marchesini, and A. A. Atienza. **Willingness to exchange health information via mobile devices: findings from a population-based survey**, *The Annals of Family Medicine*, vol. 14, no. 1, pp. 34-40, 2016.
21. S. Chai, S. Bagchi-Sen, C. Morrell, H. R. Rao, , and S. J. Upadhyaya. **Internet and online information privacy: An exploratory study of preteens and early teens**, *IEEE Transactions on Professional Communication*, vol. 52, no. 2, pp. 167-182, 2009.
22. G. Kenny. **To protect my health or to protect my health data? Examining the influence of health information privacy concerns on citizens' health technology adoption**, Doctoral dissertation, Dublin City University, 2016.
23. S. Avancha, A. Baxi, and D. Kotz. **Privacy in mobile technology for personal healthcare**. *ACM Computing Surveys*, vol. 45, no. 1, pp. 1-54, 2012. https://doi.org/10.1145/2379776.2379779
24. X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu. **Health information privacy concerns, antecedents, and information disclosure intention in online health communities**. *Information & Management*, vol. 55, no. 4, pp. 482-493, 2018.
25. B. H. Sampat, and B. Prabhakar. **Privacy risks and security threats in mHealth apps.** *Journal of International Technology and Information Management*, vol. 26, no. 4, pp. 126-153, 2017.
26. M. Plachkinova, S. Andrés, and S. Chatterjee. **A taxonomy of mhealth apps--Security and privacy concerns**, in *2015 48th Hawaii International Conference on System Sciences*, pp. 3187-3196, 2015. https://doi.org/10.1109/HICSS.2015.385
27. M. Sedek, R. Ahmad, and N. F. Othman. **Motivational Factors in Privacy Protection Behaviour Model for Social Networking.** in Proc. MATEC Web of Conferences, 2018, vol. 150, p. 05014.
28. N. F. Othman, R. Ahmad, and M. Yusoff. **Information Security and Privacy Awareness in Online Social Networks among UTeM Undergraduate Students**, *Journal of Human Capital Development*, vol. 6, no. 1, pp. 101-110, 2013.
29. J. A. Alzubi, R. Manikandan, N. Gayathri, and R. Patan. **A Survey of Specific IoT Applications**, *International Journal on Emerging Technologies*, vol. 10, no. 1, pp. 47–53, 2019.
30. K. Glanz, B. K. Rimer, and K. Viswanath, Eds. **Health behavior and health education: theory, research, and practice**. John Wiley & Sons, 2008.
31. R. W. Rogers. **A protection motivation theory of fear appeals and attitude change**, *Journal of psychology*, vol. 91, no. 1, pp. 93-114, 1975.
32. T. Dinev, V. Albano, H. Xu, A. D'Atri, and P. Hart. **Individuals' attitudes towards electronic health records: A privacy calculus perspective**, in *Advances in healthcare informatics and analytics*, Springer, 2016, pp. 19-50.
33. K. Caine, and R. Hanania. **Patients want granular privacy control over health information in electronic**

medical records, *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 7-15, 2013.

34. Y. Chen, L. Yang, M. Zhang, J. Yang. **Central or peripheral? Cognition elaboration cues' effect on users' continuance intention of mobile health applications in the developing markets**, *International journal of Medical Informatics*, vol. 116, pp. 33-45, 2018.
35. G. Bansal, and F. M. Zahedi. **Trading Trust for Discount: Does Frugality Moderate the Impact of Privacy and Security Concerns?**, in Proc. 16th Americas Conference on Information Systems, 2010, p. 417.
36. J. Melzner, J. Heinze, and T. Fritsch. **Mobile health applications in workplace health promotion: an integrated conceptual adoption framework**, *Procedia Technology*, vol. 16, pp. 1374-1382, 2014. https://doi.org/10.1016/j.protcy.2014.10.155
37. N. Mohamed, I. H. Ahmad. **Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia.** *Computers in Human Behavior*, vol. 28, no. 6, pp. 2366-2375, 2012.
38. A. C. Johnston, and M. Warkentin. **Fear appeals and information security behaviors: an empirical study**, *Management Information System Quarterly*, vol. 34, no. 3, pp. 549-566, 2010.
39. N. Salleh, R. Hussein, N. Mohamed, N. S. Abdul, A. R. Ahlan, and U. Aditiawarman. **Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory , Trust and Risk**, *Journal of Internet Social Networking & Virtual Communities*, p. 1, 2012.
40. A. Kobsa, H. Cho, and B. P. Knijnenburg. **The effect of personalization provider characteristics on privacy attitudes and behaviors: An Elaboration Likelihood Model approach**, *Journal of the Association for Information Science and Technology*, vol. 67, no. 11, pp. 2587-2606, 2016.
41. C. E. Wills, and M. Zeljkovic. **A personalized approach to web privacy: awareness, attitudes, and actions**, *Information Management & Computer Security*, vol. 19, no. 1, p. 53, 2011. https://doi.org/10.1108/09685221111115863
42. X. Guo, X. Han, X. Zhang, Y. Dang, C. Chen. **Investigating m-health acceptance from a protection motivation theory perspective: gender and age differences.** *Telemedicine and e-Health*, vol. 21, no. 8, pp. 661-669, 2015.
43. G. D. Israel. ***Sampling the evidence of extension program impact.*** Gainesville, FL: University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS, 1992.
44. L. T. Hu, and P. M. Bentler. **Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives,** *Structural equation modeling: a multidisciplinary journal*, vol. 6, no. 1, pp. 1-55, 1999. https://doi.org/10.1080/10705519909540118
45. R. Liu. **The Influence of Privacy Awareness and Privacy Self-efficacy in E-commerce**, Doctoral dissertation, University of North Carolina at Greensboro, 2015.