Pertanika J. Soc. Sci. & Hum. 33 (3): 1177 - 1196 (2025)

PERTANIKA JOURNALS

SOCIAL SCIENCES & HUMANITIES

Journal homepage: http://www.pertanika.upm.edu.my/

Concern for Information Privacy Among Internet Users in e-health Platforms

Umi Umairah Mohd Hanafi[1]*, Zuha Rosufila Abu Hasan[1], Noor Fadhiha Mokhtar[1] and Ponmalar N. Alagappar[2]

[1]Department of Management (Marketing), Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, 21300 Kuala Terengganu, Malaysia
[2]Department of Management and Marketing, Faculty of Business and Economics, Universiti Malaya, 50603 Kuala Lumpur, Malaysia

ABSTRACT

E-health platforms that utilise information technology tools have greater potential for delivering promising healthcare services to society. However, the integration of burgeoning technology leads to potential users' concerns for information privacy when using the platforms. Despite the digital health trend in seeking healthcare services through e-health platforms, the users' behavioural disposition towards e-health platforms in Malaysia remains unclear. Therefore, this study employed a quantitative research design to determine the users' attitudes toward e-health platforms. The data were collected by distributing an online questionnaire across various online platforms in Malaysia. A total of 378 valid responses from Internet users with experience in using e-health platforms were analysed using the partial least squares (PLS) algorithm and bootstrapping procedure. The findings showed that information privacy orientation was a significant predictor for all concern for information privacy (CFIP) dimensions: collection, unauthorised secondary use, improper access, and errors in e-health platforms. In addition, only the collection dimension was found to have a negative influence on users' attitudes. At the same time, the gender factor, posited as a control variable, showed no significant impact on users' attitudes towards e-health platforms. Conclusively, the findings offer significant empirical knowledge to future researchers, healthcare providers, and e-health platform developers to address the transparency over users' information collection and management to reassure users' privacy concerns in using the e-health platforms.

Keywords: CFIP, e-Health, healthcare, privacy concerns

ARTICLE INFO

Article history:
Received: 11 August 2024
Accepted: 20 December 2024
Published: 26 June 2025

DOI: https://doi.org/10.47836/pjssh.33.3.11

E-mail addresses:
u.umairahhanafi@gmail.com (Umi Umairah Mohd Hanafi)
zuha@umt. edu.my (Zuha Rosufila Abu Hasan)
noorfadhiha@umt.edu.my (Noor Fadhiha Mokhtar)
ponmalar.a@um.edu.my (Ponmalar N. Alagappar)
* Corresponding author

e-ISSN: 2231-8534

INTRODUCTION

Consistent with the technological era, the development of innovative technologies has influenced the transformation in the healthcare sector (Eysenbach, 2001). The post-COVID-19 era has witnessed e-health platforms become more prominent among society in seeking healthcare services (Pereira et al., 2023). For instance, people prefer online health consultations because they are more patient-centric (Pereira et al., 2023). On the other hand, people believe that by using e-health platforms, they can avoid overcrowding in healthcare facilities and, thus, are less likely to contract diseases from one another (Wan et al., 2020).

E-health platforms refer to the utilisation of information technology tools that provide access to healthcare services despite the geographical barriers between the users and healthcare facilities. To deliver, monitor, and store patient health information effectively, healthcare practitioners can now leverage the integration of disruptive technologies, such as big data analytics, artificial intelligence (AI), and cloud computing, into e-health platforms. Users can access e-health platforms using technological devices such as laptops and smartphones.

Among e-health services that can be accessed through these platforms are booking consultation appointments, pledging to be an organ donor, locating health facilities and specialists, ordering drug replenishments, accessing medical histories, and seeking health information. It is a norm for e-health platforms to collect and store users' information electronically over the platforms to personalise and cater to the needs of e-health platform users (Al-Ogaili et al., 2021). However, when dealing with data stored electronically, there are growing chances of the data being mismanaged and hacked by unauthorised parties. Moreover, a poorly maintained e-health platform can compromise the reliability of data. Due to the Big Data era, every piece of data is considered valuable, and healthcare records are no exception (Renugadevi et al., 2023). As reported by Alder (2023), the largest healthcare records breach occurred in 2023, involving 741 healthcare data breaches in the United States.

Esmaeilzadeh (2019, 2024) regarded health information as sensitive and private. Patients' fear of health information leaks has led to an increasing number of concerns, which may make them cautious about using e-health platforms (Esmaeilzadeh, 2019). According to Smith et al. (1996) and Adu et al. (2021), concerns among consumers are primarily attributed to a lack of control over the disclosure of personal information. Upon disclosure, users are often ignorant regarding the regulation or management of their data. As a result, they will feel deceived when their privacy is violated. Users with high privacy concerns tend to be more wary of the usage of e-health platforms. Dang et al. (2021) clarified that privacy concerns among users hinder the use of mobile health platforms, as users have become sceptical about disclosing their health information.

Despite extensive research on privacy concerns, our understanding of the influence

of privacy concerns on users' behavioural disposition in the healthcare context remains in a grey area. Adu et al. (2021) highlighted that the e-health landscape in developing countries is still in its infancy, thereby calling for additional study into privacy concerns within the healthcare context. The lack of study of privacy concerns among Malaysians in the context of e-health has emerged as the primary justification for undertaking this study, aiming to connect theoretical insights with practical understanding.

THEORETICAL FOUNDATION AND HYPOTHESIS DEVELOPMENT

Concern for Information Privacy (CFIP)

Throughout the years, a plethora of research has emerged to develop privacy concerns constructs and measurements to address the issue of privacy concerns. There are several studies on privacy concerns, including Concerns for Information Privacy (CFIP; Smith et al., 1996), Internet Users' Information Privacy Concerns (IUIPC; Malhotra et al., 2004), Internet Privacy Concerns (IPC; Dinev & Hart, 2004) and Mobile Users' Information Privacy Concerns (MUIPC; Xu et al., 2012). Among these theories, CFIP is one of the most extensively studied in multiple disciplines, including in the healthcare context (Prakash & Das, 2022; Princi & Krämer, 2020; Tseng et al., 2020). Smith et al. (1996) developed CFIP as four multidimensional constructs composed of 1) information collection (COL), 2) unauthorised secondary use (USE), 3) improper access (IMA) and 4) errors (ERR).

Previous research has shown that CFIP has good psychometric qualities that address concerns from the standpoint of the consumer (Slyke et al., 2006) and projects adaptability as a first-order construct (Stewart & Segars, 2002).

Therefore, CFIP is used in this study to examine the factors that determine users' CFIP and how those factors affect users' attitudes toward e-health platforms. CFIP served as the theoretical basis for this study by following the APCO (antecedent->privacy concerns->outcomes) macro model, as suggested by Smith et al. (2011). The model was extended by introducing information privacy orientation (IPO) as the antecedent, while attitude was posited as the outcome.

Information Privacy Orientation and CFIP

Li (2011) associated IPO as a social-psychological factor, coining the term to describe the inclination of individuals to place a higher priority on information privacy. In general, IPO reflects individuals' tendencies to protect and restrict their personal information from others (Adu et al., 2021; Li, 2011; J. F. Taylor et al., 2015). Previous study suggests that individuals with a strong propensity to safeguard and limit access to their personal information have heightened privacy concerns (Xu et al., 2011). For example, IPO is found to have a significant impact on CFIP in data collection programs (J. F. Taylor et al.,

2015). At the same time, Xu et al. (2011) found a significant correlation between IPOs and privacy concerns across four websites: e-commerce, healthcare, social networking, and finance. This suggests that individuals with a strong desire for privacy are highly likely to exhibit significant concerns about privacy. Users' privacy orientation in healthcare indicates their attitudes and behaviours concerning the protection and utilisation of their personal health information (Xu et al., 2011). However, there is only a limited number of studies that examine IPO as an antecedent to privacy concerns, particularly in developing countries, leading Adu et al. (2021) to emphasise the significance of IPO as the determinant of CFIP in the healthcare sector. Therefore, to determine the influence of IPO on privacy concerns in a healthcare context, four hypotheses were drawn:

H1a: There is a positive relationship between information privacy orientation (IPO) and concern for information privacy (CFIP) regarding information collection.

H1b: There is a positive relationship between information privacy orientation (IPO) and concern for information privacy (CFIP) regarding unauthorised secondary use.

H1c: There is a positive relationship between information privacy orientation (IPO) and concern for information privacy (CFIP) regarding improper access.

H1d: There is a positive relationship between information privacy orientation (IPO) and concern for information privacy (CFIP) regarding errors.

CFIP and Attitude

Prior research demonstrated that CFIP significantly influenced attitudes toward technology (Angst & Agarwal, 2009; Stewart & Segars, 2002; J. F. Taylor et al., 2015). In the healthcare context, attitude is the degree to which consumers' favourable or unfavourable evaluation of using e-health platforms (Hsu & Lin, 2016). Theoretically, users are likely to develop negative attitudes toward e-health platforms if they exhibit a high level of privacy concerns (Belanger & Crossler, 2019). Consequently, the likelihood of their continued engagement with the e-health platforms decreases. Tseng et al. (2020) argued that four constructs of privacy concern were believed to have a negative association with users' behavioural disposition. Therefore, based on prior literature, four hypotheses pertaining to the relationships between CFIP dimensions and users' attitudes were drawn.

(1) Information collection (COL) refers to the extent of concerns over excessive data collection by organisations (Adu et al., 2021). It is expected that information collection will have a negative influence on users' attitudes towards e-health platforms. Therefore, a hypothesis was drawn;

H2a: There is a negative relationship between concerns for information privacy (CFIP) regarding information collection and users' attitudes towards e-health platforms.

(2) Unauthorised secondary use (USE) refers to the degree of concern towards unauthorised secondary purposes other than the consented purpose by the users (Adu et al., 2021). It is expected that information collection will have a negative influence on users' attitudes towards e-health platforms. Therefore, a hypothesis was drawn:

H2b: There is a negative relationship between concerns for information privacy (CFIP) regarding unauthorised secondary use and users' attitudes towards e-health platforms.

(3) Improper access (IMA) refers to the degree of concern regarding organisations' inability to safeguard consumers' personal information against improper access (Adu et al., 2021). It is expected that improper access will negatively influence users' attitudes towards e-health platforms. Therefore, a hypothesis was drawn:

H2c: There is a negative relationship between concerns for information privacy (CFIP) regarding improper access and users' attitudes towards e-health platforms.

(4) Errors (ERR) refers to the degree of concern towards inadequate data protection against errors in users' personal information (Adu et al., 2021). It is expected that errors will negatively influence users' attitudes towards e-health platforms. Therefore, a hypothesis was drawn:

H2d: There is a negative relationship between concerns for information privacy (CFIP) regarding errors and users' attitudes towards e-health platforms.

Control Variable

A general demographic control variable, gender, was used. A control variable aids in explaining variation in a dependent variable (DV) by taking into account factors aside from the main theoretical constructs in the study (Ngah et al., 2017). The impact of gender as a control variable has been extensively researched in prior research (Esmaeilzadeh, 2019, 2024; Pereira et al., 2023). It is believed that consumers' attitudes toward e-health platforms and their degree of privacy concerns vary depending on their gender.

METHODS

Study Design and Procedure

A quantitative research method was employed by distributing the questionnaire throughout the online platforms. Multiple online platforms were utilised to cover a wide geographical area of questionnaire distribution in Malaysia. A purposive sampling approach was adopted, where recruitment criteria were established for selection. The respondents' inclusion criteria for this study were Malaysian Internet users aged 18 years or older who have experience using e-health platforms. A minimum age was imposed because e-health platform users have to be at least 18 years old to register for the platform individually. In

Malaysia, individuals aged 18 years or older are regarded as consenting adults.

Study Participants and Sampling

The respondents should have experience with e-health platforms to determine their attitude towards the usage of e-health platforms. A total of 378 valid questionnaire responses were collected. The number of responses was considered adequate, and the sample sizes ranging from 200 to 400 are optimal for SEM analysis (Oke et al., 2012).

Study Instruments

Privacy concern instruments were adapted from CFIP instruments developed by Stewart and Segars (2002) and IPO instruments presented in the works of Xu et al. (2011) and J. F. Taylor et al. (2015). Attitude instruments were derived from J. F. Taylor et al. (2015) and S. Taylor and Todd (1995). Self-developed items were added to CFIP instruments to enhance and cover the context of the research, while other questions were adapted accordingly. The questionnaire instruments underwent a pre-testing procedure by academic experts. Based on the experts' feedback, changes were made to the questionnaires before actual data collection.

Structure of the Questionnaire

The questionnaire consists of two sections: Section A, which covers the demographics of the respondents, and Section B, which includes IPO items. The CFIP dimensions (COL, USE, IMA, ERR) items are covered in Sections C, D, E, and F, respectively. Last but not least, attitude measurement instruments were covered in section G. A 5-point Likert scale, measured from 1 to 5 (strongly disagree to strongly agree), was employed since it is a common universal scale; thus, the 5-point Likert scale conveyed familiarity to respondents in expressing their answer (Bessenyei et al., 2021).

Data Analysis Tools

In this study, two statistical software packages were employed: SPSS for data cleaning and preparation, as well as descriptive statistical analysis and SmartPLS for the analysis of measurement and structural models. The data was examined using SPSS for consistency and the presence of missing data, while straight-lining responses and outliers were eliminated to maintain data integrity (Aldrich & Cunningham, 2016). Descriptive statistics were subsequently performed to determine the demographics of the respondents. Following this, the data was exported to SmartPLS for additional analysis. The measurement model analysis was performed to assess the reliability and validity of the data (Table 3). Hair et al. (2017) indicate that the data must demonstrate acceptable cut-off values for reliability and validity tests before advancing to the structural model analysis. The correlations and relationships among the factors were subsequently analysed through the PLS-SEM technique in the structural model analysis.

Ethical Aspects

Prior to distributing the questionnaires, this study obtained ethics approval from the ethical committee at the Research

Management and Innovation Centre (RMIC) at Universiti Malaysia Terengganu. The committee approved the distribution of the survey questionnaires, ensuring there would be no further repercussions. Participants were made aware that their involvement was entirely voluntary, that the data would be treated confidentially, and that it would solely be utilised for this study while ensuring their identities remained anonymous throughout the survey. In line with ethical research practices, informed consent was obtained from all individuals prior to their participation. The individual also emphasised that participants were free to withdraw from the survey if they felt any discomfort or changed their minds. Incomplete questionnaires were not retained and were entirely removed from the data set. While the study's context focused on privacy concerns, the respondents were assured that the profiling questions were limited to general inquiries regarding age, gender, education, and usage features of e-health platforms. Figure 1 highlights the research framework for this study.

RESULTS

Descriptive Analysis Using SPSS Version 26.0

Table 1 illustrates that the demographic profile of respondents consisted of 42.3% male participants, while females accounted for the remaining 57.7%. The gender distribution was quite balanced, considering the small difference between the two genders. In terms of age, the majority of respondents were aged 27–42 (49.21%), followed by those aged 18–26 (45.24%), and 5.0% of respondents were aged 43–58 years old. However, only 0.5% of respondents were aged 59 years and above. Most respondents can be seen to be from the younger and millennial generations, considering their association characteristics as heavy users of digital technology, in contrast to elders who tend to spend less time on the Internet (Wan et al., 2020). This is in line with the Malaysian Communications and Multimedia Commission (2022), which reported that Malaysians aged 60 years old

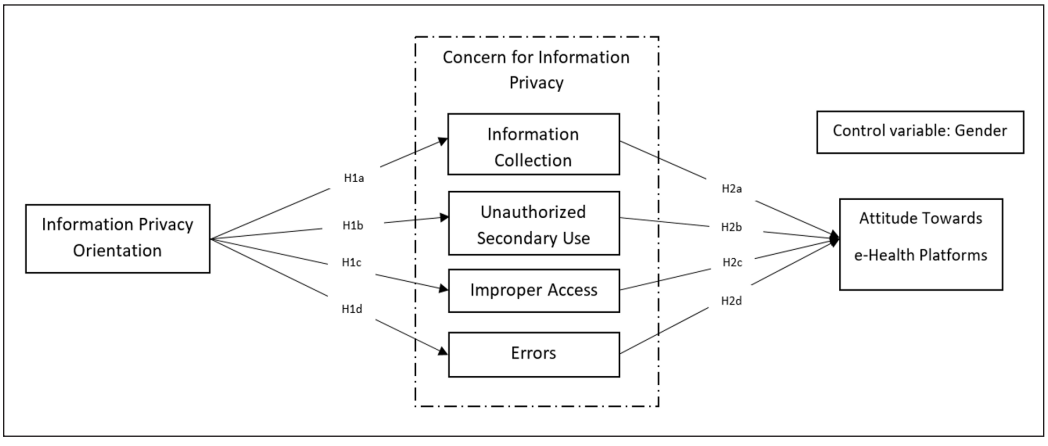

Figure 1. Research model

Table 1
Demographic profile respondents

Demographic Variable	Age range	N = 378	Percentage (%)
Age	18-26	171	45.24
	27-42	186	49.21
	43-58	19	5.0
	59 and above	2	0.53
	Total:	378	100.0%
Gender	Male	160	42.3
	Female	218	57.7
	Total:	378	100.0%

and above are mostly non-Internet users, thus reflecting the minority response in this study. Therefore, the sample distribution in this study can be considered reasonable.

To understand the usage of e-health platforms, the respondents were asked about their use of the platforms' features. Accordingly, 61.1% of respondents agreed that they mostly use e-health platforms to seek the latest health information. In comparison, 51.9% of respondents tend to book health screening appointments beforehand to avoid overcrowding at health facilities. Considerably, 37.6% of respondents prefer to book online appointments. Other uses of e-health platforms, such as locating nearby specialists and facilities, replenishing medicine, and updating and reviewing their health status, were also reported by the respondents.

Measurement Model Assessments Using SmartPLS Version 4.0

For this research, the measurement model assessments for the reflective constructs were conducted, including internal consistency reliability, individual indicator reliability, convergent validity and discriminant validity (Hair et al., 2017, 2019). The internal consistency reliability was assessed using both Cronbach's alpha and composite reliability. Table 2 indicates that the values for all constructs regarding Cronbach's alpha and composite reliability exceeded 0.80, signifying excellent reliability, as the acceptable threshold for both evaluations is over 0.70 (Hair et al., 2020).

As for the validity assessments, the factor loadings and average variance extracted (AVE) were examined. The factor loadings for all items in the constructs varied from 0.639 to 0.890, exceeding the minimum threshold value of 0.4 established by Hair et al. (2017). The AVE values for the constructs were reported to exceed the acceptable cut-off value, which is 0.5 (Hair et al., 2019). The lowest AVE value, as highlighted in Table 3, showed that IPO (AVE=0.597), COL (AVE=0.638), USE (AVE=0.645), IMA (AVE=0.641), ERR (AVE=0.648) and ATT (AVE=0.664). Overall, all constructs exhibited adequate convergent validity, as shown in Table 2.

Table 2
Measurement model analysis

Constructs	Items	Convergent Validity		Internal consistency reliabilities	
		Loadings	AVE>0.5	Cronbach's alpha	CR
IPO	IPO1	0.696	0.597	0.830	0.881
	IPO2	0.738			
	IPO3	0.806			
	IPO4	0.829			
	IPO5	0.788			
CFIP-COL	COL1	0.846	0.638	0.903	0.924
	COL2	0.829			
	COL3	0.890			
	COL4	0.866			
	COL5	0.786			
	COL6	0.655			
	COL7	0.685			
CFIP-USE	USE1	0.639	0.645	0.888	0.915
	USE2	0.790			
	USE3	0.842			
	USE4	0.855			
	USE5	0.839			
	USE6	0.833			
CFIP-IMA	IMA1	0.742	0.641	0.887	0.914
	IMA2	0.827			
	IMA3	0.867			
	IMA4	0.806			
	IMA5	0.831			
	IMA6	0.723			
CFIP-ERR	ERR1	0.798	0.648	0.891	0.917
	ERR2	0.855			
	ERR3	0.834			
	ERR4	0.825			
	ERR5	0.715			
	ERR6	0.796			
ATT	ATT1	0.816	0.664	0.899	0.922
	ATT2	0.850			
	ATT3	0.818			
	ATT4	0.782			
	ATT5	0.793			
	ATT6	0.828			

Note. CFIP = concern for information privacy (CFIP); IPO = information privacy orientation; COL = collection; USE = unauthorised secondary use; IMA = improper access; ERR = errors; ATT = attitude

Afterwards, discriminant validity was examined by using HTMT. Table 3 reported that all the HTMT values were less than 1.0 (Henseler et al., 2015), indicating that the constructs were distinct from each other. Based on the results, this study demonstrated satisfactory reliability and validity values for all research constructs. Therefore, no item removal was reported, and all items were retained for subsequent structural model assessments.

Structural Model Assessments

This study followed the steps outlined by Hair et al. (2017) in conducting structural model assessments. Prior to structural model assessment, the variance inflation factor (VIF) values were evaluated for each construct to ensure that the regression result is free from collinearity issues. No collinearity issues were reported, as all VIF values were below the threshold value of 5.

The structural model assessments were conducted by using a bootstrapping procedure, as suggested by Hair et al. (2017). The one-tailed test was chosen since the hypotheses were developed with directional paths (Kock, 2015). Therefore, the procedure was set with a significance level of 0.05, a one-tailed test, and 5,000 subsamples (Hair et al., 2017).

Based on the findings, five out of eight hypotheses proposed were supported. Firstly, the impact of gender, as a control variable, on users' attitudes towards e-health platforms was tested. The result revealed that gender (β = 0.060, *t*-value = 0.648, *p*-value >0.05) did not significantly influence consumers' attitudes towards e-health platforms.

Four hypotheses that were developed based on IPO relationships with four dimensions of CFIP (COL, USE, IMA and ERR) were supported. IPO is found to have a significant positive influence on concern for information privacy (CFIP) regarding information collection (COL), unauthorised secondary use (USE), improper access (IMA) and errors (ERR). The results showed that hypothesis H1a, IPO->COL (β = 0.316, *t*-value = 6.935, *p*-value ≤0.05), hypothesis H1b, IPO->USE (β = 0.436, *t*-value =7.588, *p*-value ≤0.05), hypothesis

Table 3
Discriminant validity of the constructs

	ATT	ERR	IMA	USE	COL	IPO
ATT						
ERR	0.534					
IMA	0.309	0.724				
USE	0.309	0.672	0.921			
COL	0.109	0.204	0.326	0.296		
IPO	0.240	0.481	0.492	0.505	0.365	

Note. IPO = information privacy orientation; COL = collection; USE = unauthorised secondary use; IMA = improper access; ERR = errors; ATT = attitude

H1c, IPO->IMA (β = 0.424, *t*-value =7.748, *p*-value ≤0.05) and hypothesis H1d, IPO->ERR (β = 0.414, *t*-value = 8.148, *p*-value ≤0.05). Therefore, hypotheses H1a to H1d were supported, indicating a positive and significant influence of users' IPO on COL, USE, IMA, and ERR.

For the CFIP dimensions, only concern about COL was found to be negatively significant with users' attitudes. Thus, hypothesis H2a, COL->ATT (β = -0.184, *t*-value = 4.350, *p*-value ≤0.05) was supported. Interestingly, the findings revealed H2b, USE->ATT (β = 0.078, *t*-value =1.008, *p*-value >0.05), H2c, IMA->ATT (β = -0.051, *t*-value = 0.665, *p*-value >0.05) and H2d, ERR->ATT (β = 0.509, *t*-value =8.375, *p*-value <0.05), indicating H2b, H2c and H2d hypotheses were not supported.

In terms of the model's explanatory power (R^2), the model was found to explain 27.2% of the variance for users' attitudes towards e-health platforms. In social science research, Ozili (2023) claimed that the (R^2) value between 10% and 50% is acceptable if most of the explanatory variables in the model are statistically significant. Based on the findings, the explanatory power of this model was deemed acceptable. In addition, the effect size analysis (f^2) was conducted to evaluate the significant influence of exogenous constructs on endogenous constructs (Hair et al., 2017). Subsequently, the findings revealed that f^2 of IPO on COL (H1a) was small, while IPO on USE (H1b), IMA (H1c) and ERR (H1d) were medium in size, respectively. On the other hand, f^2 of COL on ATT (H2a) was also found to have a small effect size. Meanwhile, no effect sizes were reported for H2b, H2c and H2d. Table 4 reports the findings for hypothesis testing, VIF and f^2 of the study, whereas Figure 2 depicts the summary of the structural model results.

Table 4
Structural model analysis

Hypo	R/ship	(β)	Std. Error	*T*-value	*P*-value	Decision	VIF	f^2
H_{1a}	IPO->COL	0.316	0.046	6.935	0.000	Supported	1.000	0.111
H_{1b}	IPO->USE	0.436	0.057	7.588	0.000	Supported	1.000	0.234
H_{1c}	IPO->IMA	0.424	0.055	7.748	0.000	Supported	1.000	0.219
H_{1d}	IPO->ERR	0.414	0.051	8.148	0.000	Supported	1.000	0.207
H_{2a}	COL->ATT	-0.184	0.042	4.350	0.000	Supported	1.095	0.043
H_{2b}	USE->ATT	0.078	0.077	1.008	0.157	Not supported	3.106	-
H_{2c}	IMA->ATT	-0.051	0.076	0.665	0.253	Not supported	3.491	-
H_{2d}	ERR->ATT	0.509	0.061	8.375	0.000	Not supported	1.771	-
-	Gender ->ATT	0.060	0.092	0.648	0.258	-	-	-

Note. IPO = information privacy orientation; COL = collection; USE = unauthorised secondary use; IMA = improper access; ERR = errors; ATT = attitude

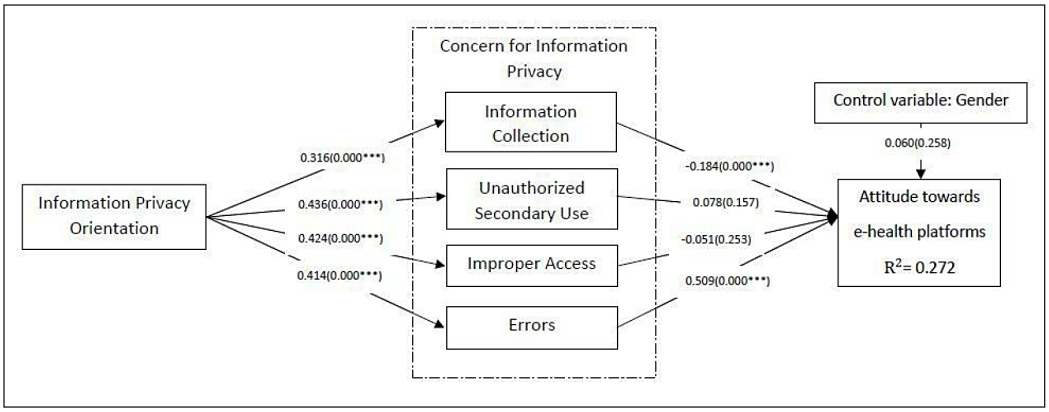

Figure 2. Structural model results
Note. *p<0.10, **p<0.05, ***p<0.001

DISCUSSIONS

This study explored the determinants of CFIP and the relationship between users' privacy concerns and attitudes by extending the CFIP model with IPO and ATT. The findings indicated that IPO significantly influenced four dimensions of CFIP (COL, USE, IMA, ERR), thus supporting hypotheses H1a, H1b, H1c and H1d. The findings are consistent with prior studies, indicating that the higher the disposition of e-health platform users in guarding their information privacy, the greater privacy concerns will be reflected (Adu et al., 2021; Xu et al., 2011). This can be seen when the IPO was found to positively influence users' concerns regarding information privacy, specifically in terms of (1) information collection concern, (2) unauthorised secondary use concern, (3) improper access concern, and (4) data error concern, in the e-health platform context.

Li (2011) categorised IPO as one of the psychological factors; hence, it is possible that when e-health platform users perceive health information as highly discreet, they will be more guarded in disclosing their information. For instance, Esmaeilzadeh (2019, 2024) emphasised that health information is considered personal and confidential, as it illustrates users' health status. Users may be aware of the potential risks associated with the improper handling of health information when engaging with the platform. Based on the contemplation of the possible risks and benefits of information disclosure on e-health platforms, users decide which information to disclose and which to withhold (Kharlamov et al., 2023). As such, users' privacy orientation in the healthcare setting may have been psychologically impacted by the recognition of the potentially serious implications of mishandling health records, such as incorrect diagnoses, errors in the prescriptions of medications, and potentially fatal effects. This can be seen in Xu et al. (2011), who found that consumers consider healthcare websites to be riskier than e-commerce, financial, and social networking sites.

Consequently, users ought to reflect on their privacy orientation as revealed in all four aspects of privacy concerns. In regard to the relationship between CFIP dimensions and users' attitudes towards e-health platforms, only COL was found to be negatively significant towards users' ATT. The outcome supported the H2a hypothesis. The result is consistent with Hwang et al. (2012), emphasising that the general public had voiced their concerns over information collection by healthcare facilities. Based on the findings, the users who have concerns pertaining to information collection will negatively influence their attitude towards e-health platforms. Perchance, the frequent collection of personal information from different healthcare practices in Malaysia played a vital role in triggering the users' concern about COL. The lack of an integrated database of patient information among healthcare facilities has become a critical issue faced by Malaysian healthcare facilities (Ministry of Health Malaysia, 2021). Inevitably, it contributes to information management issues in healthcare settings. This prompts e-health platforms to acquire users' personal health information separately and store it in a separate database, causing data redundancy and inconsistencies. The prolonged issue may compromise users' data integrity, consequently heightening users' concerns regarding information collection in healthcare settings.

Interestingly, no relationship was found between USE and IMA dimensions and users' attitudes towards e-health platforms. Hypotheses H2b and H2c were not supported. This is counterintuitive with past studies (Esmaeilzadeh, 2019; Hwang et al., 2012; Mwesiumo et al., 2021) that predicate concerns for unauthorised secondary use and improper access are highly significant to users' behavioural disposition. The probable reason behind the findings would be due to a lack of awareness regarding information privacy practices among healthcare providers. Malhotra et al. (2004) defined awareness as the extent to which a consumer is concerned about organisational information practices. In exchange for health services, most users of e-health platforms will provide necessary details without a clear understanding of how their data will be secured. Nevertheless, upon data disclosure, users are predominantly unaware of the electronic management of their data (Adu et al., 2021). Fox and James (2021) debated that most users portrayed scepticism regarding the potential for unauthorised secondary use and improper access, as they 'assumed' that the information provided was solely utilised for their treatment, reflecting a lack of awareness concerning the misuse and mishandling of health information by the organisation. For example, the rumours over changes in management that operate the national e-health platform, MySejahtera, had left Malaysians baffled (Malik, 2022). The hashtag #StopUsingMySejahtera on social media platforms has gone viral, showing growing concerns among Malaysians over the potential misuse of their health information (Krishnan, 2022). Therefore, it is essential for healthcare providers and e-health platform management to maintain

transparency about their privacy practices to address and alleviate privacy concerns among users of e-health platforms.

Interestingly, concerns for errors depicted a significant positive relationship with users' ATT. This is in contradiction with H2d's proposed direction. Thus, H2d is not supported. Personal health information errors are unavoidable due to human and technological errors. However, such errors can cause misdiagnoses and inappropriate treatment plans (Esmaeilzadeh, 2019). The findings demonstrated that Malaysians acknowledged the concerns over errors. However, it does not negatively affect their attitudes towards e-health platforms. A possible explanation is that Malaysian users might exhibit higher trust in healthcare practitioners regarding the verification of health information. This may be attributed to the establishment of a dual-tiered healthcare system in Malaysia, which the government oversees. Raschke et al. (2014) asserted that citizens have higher trust in services that are overseen by the government, believing that the government will hold service providers accountable for any issues that arise. This is corroborated by Earp and Payton (2006), who noted that healthcare personnel express significant concerns regarding inaccuracies in patient information. In addition, the integration of disruptive technologies in e-health platforms can also reduce data omission errors compared to manual data entry (Angst & Agarwal, 2009; Bates, 2000). Any inaccuracy in personal health information can be easily detected by the AI, thus reducing the presence of information errors in the information system. Accordingly, users believe that healthcare practitioners will adequately rectify any potential errors before formulating medical diagnoses, thus reinforcing users' positive attitudes towards e-health platforms.

To reduce users' concerns regarding information errors in e-health platforms, platform providers could grant access to users' medical records. This enables users to verify the accuracy of their health records and promptly notify healthcare practitioners of potential errors that could compromise future medical diagnoses. For example, Italy has given its citizens the autonomy to access their medical records and histories digitally through e-health platforms (Sarabdeen & Moonesar, 2017).

CONCLUSION

Conclusively, this study explored the relationship between individuals' disposition in guarding their information privacy and privacy concerns and how it affects users' attitudes towards e-health platforms. The IPO significantly influenced all four dimensions of CFIP: COL, USE, IMA, and ERR. However, it seems that concerns regarding information collection are the sole dimension impacting users' attitudes toward e-health platforms in Malaysia. This suggests that users' desire for information privacy can influence their privacy concerns, with only the collection (COL) dimension showing a significant negative impact on attitudes towards these platforms. The finding highlights the concerns among

Malaysians regarding the extensive collection of personal information practices by healthcare providers in Malaysia. In addition, the findings also revealed that the other proposed dimensions of CFIP—unauthorised secondary use (USE), improper access (IMA), and errors (ERR)—were not supported. In a similar vein, gender, which served as the control variable for users' attitudes, was found to be insignificant, indicating that users' attitudes toward e-health platforms remain unaffected by their gender.

Implications for Theory and Practice

This study contributes to the body of knowledge by exploring privacy concerns within the healthcare context and examining users' attitudes in both theoretical and practical implications. Theoretically, the findings from this study provide deeper insights into the employment of the APCO macro model in privacy concern studies. Firstly, the findings reaffirmed the IPO roles as the antecedent of privacy concerns in the healthcare context, as discussed in prior literature. This shows the consistency of individuals' privacy orientation that will affect their privacy concerns, especially when it involves sensitive and confidential information. Therefore, this finding contributes theoretically by bridging the critical gap over the lack of existing studies that address the influence of IPO on privacy concerns in the healthcare context, especially in developing countries (Adu et al., 2021).

Secondly, positioning CFIP as the first-order model is the right call since it allows the researcher to discover that the collection dimension is highly associated with the Malaysian healthcare environment compared to unauthorised secondary use, improper access and errors. The findings proved that CFIP dimensions were projected differently, as debated earlier by Stewart and Segars (2002). Thirdly, the findings also reaffirm the strong association of privacy concerns towards users' behavioural disposition. Behavioural disposition has been discussed as the outcome of privacy concerns in multiple literature (Li, 2011; Shen et al., 2019).

In terms of practical implications, healthcare providers and e-health platform developers should address the transparency over information collection and its usage in e-health platforms to reassure users to provide their information in exchange for e-health services. The extensive collection of data, particularly on several platforms, can increase anxiety among users, especially when it involves sensitive health information. Moreover, healthcare providers and e-health platform management should also follow the rules and regulations implemented by the Malaysian government in protecting and preserving data integrity from illegal means to reassure the users of the cybersecurity safety in using e-health platforms (Zishan et al., 2019). Cautiousness over information reliability can influence users' prolonged attitude towards the platforms. Although the usage of e-health platforms provides several benefits to Malaysian users, the risks of having to jeopardise users' personal information in exchange for e-health services

might hinder Malaysian acceptance of fully utilising e-health platforms.

Study Limitations and Future Research Directions

Undoubtedly, this finding extends insights into privacy concerns in the healthcare context. However, there are several limitations that limit the generalizability of the findings. The first limitation acknowledged is primarily based on the sample population. The cohort was heavily biased towards respondents aged 18 and 58 years old, depicting a lack of respondents from those aged 59 and above. Therefore, future research could administer systematic ways to minimise the response bias from respondents' population ages (Esmaeilzadeh, 2024). This is because the utilisation of e-health platforms is beneficial to both younger generations and the elderly in seeking e-health services from the comfort of their own homes.

Besides that, the findings from this study are limited to one determinant. According to our findings, the models explained 27.2% of the variance in users' attitudes. Perhaps adding other potential variables can increase the explanatory power of the research model. Future research can extend the CFIP research framework by integrating the privacy calculus theory (Dinev & Hart, 2004). It is interesting to look into how users decide to share their information on an e-health platform based on the perceived risks and benefits involved. In terms of technology adoption, the Technology Acceptance Model (TAM; Davis, 1989) or the Unified Theory of Acceptance and Use of Technology (UTAUT; Venkatesh et al., 2003) could also be integrated into the existing framework (Dhagarra et al., 2020). Both theories are frequently utilised in the literature to determine users' acceptance of new technology; hence, it is noteworthy to examine users' acceptance of e-health platforms in Malaysia. This study will benefit the researchers, but e-health platform developers will also learn about users' behavioural patterns when utilising the platform.

ACKNOWLEDGEMENTS

The authors thank all participants for their valuable contributions and the academic supervisors for their guidance and support. Last but not least, sincere thanks are extended to the reviewers for their thoughtful suggestions and constructive feedback, which significantly enhanced the quality of this paper.

REFERENCES

Adu, E. K., Mills, A., & Todorova, N. (2021). Factors influencing individuals' personal health information privacy concerns. A study in Ghana. *Information Technology for Development*, *27*(2), 208-234. https://doi.org/10.1080/02681102.2020.1806018

Alder, S. (2023, Jun 20). *Healthcare data breach statistics*. HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Aldrich, J. O., & Cunningham, J. B. (2016). *Using IBM SPSS statistics: An interactive hands-on approach* (2nd ed.). Sage Publications.

Al-Ogaili, A. S., Alhasan, A., Ramasamy, A., Marsadek, M., Hashim, T. J. T., Al-Sharaa, A., Aadam, M., & Audah, L. (2021). IoT technologies for tackling COVID-19 in Malaysia and worldwide: Challenges, recommendations, and proposed framework. *Computers, Materials and Continua*, *66*(2), 2141-2164. https://doi.org/10.32604/cmc.2020.013440

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *Mis Quarterly*, *33*(2), 339-370. https://doi.org/10.2307/20650295

Bates, D. W. (2000). Using information technology to reduce rates of medication errors in hospitals. *British Medical Journal*, *320*(7237), 788-791. https://doi.org/10.1136/bmj.320.7237.788

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems*, *28*(1), 34-49. https://doi.org/10.1016/j.jsis.2018.11.002

Bessenyei, K., Suruliraj, B., Bagnell, A., McGrath, P., Wozney, L., Huguet, A., Elger, B. S., Meier, S., & Orji, R. (2021). Comfortability with the passive collection of smartphone data for monitoring of mental health: An online survey. *Computers in Human Behavior Reports*, *4*, Article 100134. https://doi.org/10.1016/j.chbr.2021.100134

Dang, Y., Guo, S., Guo, X., Wang, M., & Xie, K. (2021). Privacy concerns about health information disclosure in mobile health: Questionnaire study investigating the moderation effect of social support. *JMIR MHealth and UHealth*, *9*(2), Article e19594. https://doi.org/10.2196/19594

Davis, F. D., (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *International Journal of Medical Informatics*, *141,* Article 104164. https://doi.org/10.1016/j.ijmedinf.2020.104164

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour and Information Technology*, *23*(6), 413-422. https://doi.org/10.1080/01449290410001715723

Earp, J. B., & Payton, F. C. (2006). Information privacy in the service sector: An exploratory study of health care and banking professionals. *Journal of Organizational Computing and Electronic Commerce, 16*(2), 105-122. https://doi.org/10.1207/s15327744joce1602_2

Esmaeilzadeh, P. (2019). The effects of public concern for information privacy on the adoption of health information exchanges (HIEs) by healthcare entities. *Health Communication*, *34*(10), 1202-1211. https://doi.org/10.1080/10410236.2018.1471336

Esmaeilzadeh, P. (2024). Privacy concerns about sharing general and specific health information on Twitter: Quantitative study. *JMIR Formative Research*, *8*(1), Article e45573. https://doi.org/10.2196/45573

Eysenbach, G. (2001). What is e-health? *Journal of Medical Internet Research*, *3*(2), 1-5. https://doi.org/10.2196/jmir.3.2.e20

Fox, G., & James, T. L. (2021). Toward an understanding of the antecedents to health information privacy concern: A mixed methods study. *Information Systems Frontiers*, *23*(6), 1537-1562. https://doi.org/10.1007/s10796-020-10053-0

Hair, J. F. J., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on Partial Least Squares Structural Equation Modeling (PLS-SEM;* 2nd ed.) Sage Publications.

Hair, J. F., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-

SEM using confirmatory composite analysis. *Journal of Business Research*, *109*, 101-110. https://doi.org/10.1016/j.jbusres.2019.11.069

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516-527. https://doi.org/10.1016/j.chb.2016.04.023

Hwang, H. G., Han, H. E., Kuo, K. M., & Liu, C. F. (2012). The differing privacy concerns regarding exchanging electronic medical records of internet users in Taiwan. *Journal of Medical Systems*, *36*(6), 3783-3793. https://doi.org/10.1007/s10916-012-9851-1

Kharlamov, A., Hohmann, R., & Parry, G. (2023). Data sharing decisions: Perceptions and intentions in healthcare. *Strategic Change*, *32*(6), 223-237. https://doi.org/10.1002/jsc.2558

Kock, N. (2015). One-tailed or two-tailed P values in PLS-SEM? *International Journal of E-Collaboration*, *11*(2), 1-7. https://doi.org/10.4018/ijec.2015040101

Krishnan, B. D. (2022, March 27). #StopUsingMySejahtera gaining traction on Twitter. *New Straits Time*. https://www.nst.com.my/news/nation/2022/03/783612/stopusingmysejahtera-gaining-traction-twitter

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 453-496. https://doi.org/10.17705/1cais.02828

Malaysian Communications and Multimedia Commission. (2022). *Internet Users Survey 2022*. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018-(Infographic).pdf

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355. https://doi.org/10.1287/isre.1040.0032

Malik, M. A. (2022, March 27). MySejahtera tidak dijual kepada swasta, kerahsiaan terjamin [MySejahtera is not sold to private entities, confidentiality is guaranteed]. *Harian Metro.* https://www.hmetro.com.my/utama/2022/03/825647/mysejahtera-tidak-dijual-kepada-swasta-kerahsiaan-terjamin

Ministry of Health Malaysia. (2021). *National Policy for Quality in Healthcare*. http://library.nih.gov.my/e-doc/flipbook/npqh20222026/index.html

Mwesiumo, D., Halpern, N., Budd, T., Suau-Sanchez, P., & Bråthen, S. (2021). An exploratory and confirmatory composite analysis of a scale for measuring privacy concerns. *Journal of Business Research*, *136*, 63-75. https://doi.org/10.1016/j.jbusres.2021.07.027

Ngah, A. H., Zainuddin, Y., & Thurasamy, R. (2017). Applying the TOE framework in the halal warehouse adoption study. *Journal of Islamic Accounting and Business Research, 8*(2), 161-181. https://doi.org/10.1108/JIABR-04-2014-0014

Oke, A. E., Ogunsami, D. R., & Ogunlana, S. (2012). Establishing a common ground for the use of structural equation modelling for construction related research studies. *Australasian Journal of Construction Economics and Building*, *12*(3), 89-94. https://doi.org/10.5130/ajceb.v12i3.2658

Ozili, P. K. (2023). The acceptable R-Square in empirical modelling for social science research. In C. A. Saliya (Ed.), *Social research methodology and publishing results: A guide to non-Native English speakers* (pp. 134-143). IGI Global Scientific Publishing. https://doi.org/10.2139/ssrn.4128165

Pereira, F. V., Tavares, J., & Oliveira, T. (2023). Adoption of video consultations during the COVID-19 pandemic. *Internet Interventions*, *31,* Article 100602. https://doi.org/10.1016/j.invent.2023.100602

Prakash, A. V., & Das, S. (2022). Explaining citizens' resistance to use digital contact tracing apps: A mixed-methods study. *International Journal of Information Management*, *63,* Article 102468. https://doi.org/10.1016/j.ijinfomgt.2021.102468

Princi, E., & Krämer, N. C. (2020). Out of control – Privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Frontiers in Psychology, 11,* Article 582054. https://doi.org/10.3389/fpsyg.2020.582054

Raschke, R. L., Krishen, A. S., & Kachroo, P. (2014). Understanding the components of information privacy threats for location-based services. *Journal of Information Systems*, *28*(1), 227-242. https://doi.org/10.2308/isys-50696

Renugadevi, N., Saravanan, S., & Naga Sudha, C. M. (2023). Revolution of smart healthcare materials in big data analytics. *Materials Today: Proceedings*, *81*, 834-841. https://doi.org/10.1016/j.matpr.2021.04.256

Sarabdeen, J., & Moonesar, I. A. (2017). Privacy protection laws and public perception of data privacy: The case of Dubai e-Health care services. *Benchmarking: An International Journal*, *25*(6), 1883-1902. https://doi.org/10.1108/BIJ-06-2017-0133

Shen, N., Bernier, T., Sequeira, L., Strauss, J., Pannor, M., Carter-Langford, A., & Wiljer, D. (2019). Understanding the patient privacy perspective on health information exchange: A systematic review. *International Journal of Medical Informatics*, *125*, 1-12. https://doi.org/10.1016/j.ijmedinf.2019.01.014

Slyke, C. V., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 415-444. https://doi.org/10.17705/1jais.00092

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdiscplinary review. *MIS Quarterly*, *35*(4), 989-1015. https://doi.org/10.2307/41409970

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167-196. https://doi.org/10.2307/249477

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36-49. https://doi.org/10.1287/isre.13.1.36.97

Taylor, J. F., Ferguson, J., & Ellen, P. S. (2015). From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing*, *32*(2), 99-112. https://doi.org/10.1108/JCM-07-2014-1078

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*. *6*(2), 144-176.

Tseng, H. T., Hung, W. F., Hwang, H. G., & Chang, I. C. (2020). Do patients' privacy concerns influence their intention toward medical image exchange consent in Taiwan? *Healthcare, 8*(1), Article 14. https://doi.org/10.3390/healthcare8010014

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis F. D. (2003). User acceptance of information technology: Toward a unified view.

MIS Quarterly, 27(3), 425-478. https://doi.org/10.2307/30036540

Wan, Y., Zhang, Y., & Yan, M. (2020). What influences patients' willingness to choose in online health consultation? An empirical study with PLS–SEM. *Industrial Management and Data Systems*, *120*(12), 2423-2446. https://doi.org/10.1108/IMDS-11-2019-0633

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824. https://doi.org/10.17705/1jais.00281

Xu, H., Gupta, S., Rosson, M. B., & Caroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the International Conference on Information Systems, ICIS 2012* (pp. 2278-2293).

Zishan, M. S. R., Hossain, C. A., Mohamed, M. A., & Sharun, S. M. (2019). The scenario of e-Health systems in developing countries (Bangladesh and Malaysia). *International Journal of Recent Technology and Engineering*, *8*(1C2), 636-641. https://doi.org/10.5958/0976-5506.2019.00573.4