International Journal of Healthcare Technology and Management

ISSN online: 1741-5144 - ISSN print: 1368-2156
https://www.inderscience.com/ijhtm

An empirical study of healthcare professionals' willingness to utilise telehealth services based on protection motivation theory

Jonathan Kissi, Baozhen Dai, Emmanuel Kusi Achmpong, Alex Boadi Dankyi, Joseph Antwi

DOI: 10.1504/IJHTM.2022.10052773

Article History:

Received:	11 June 2021
Accepted:	24 March 2022
Published online:	17 April 2023

An empirical study of healthcare professionals' willingness to utilise telehealth services based on protection motivation theory

Jonathan Kissi*

School of Allied Health Sciences,
Department of Health Information Management,
University of Cape Coast,
University Post Office,
Cape Coast, Ghana
Email: jonathan.kissi@ucc.edu.gh
*Corresponding author

Baozhen Dai

Department of Health Policy and Management,
Jiangsu University, School of Management,
301 Xuefu Road, Zhenjiang, 212013, China
Email: hixiaodai@126.com

Emmanuel Kusi Achmpong

School of Allied Health Sciences,
Department of Health Information Management,
University of Cape Coast,
University Post Office,
Cape Coast, Ghana
Email: eachampong@ucc.edu.gh

Alex Boadi Dankyi

Department of Research and Innovations,
University of Cape Coast,
Cape Coast, Ghana
Email: joesph.antwi@ucc.edu.gh

Joseph Antwi

School of Allied Health Sciences,
Department of Health Information Management,
University of Cape Coast,
University Post Office,
Cape Coast, Ghana
Email: joesph.antwi@ucc.edu.gh

Abstract: With the increasing data protection regulations, protecting patients' digital information is a growing concern for healthcare professionals and institutions, as people continuously live their lives through telehealth services. This study examines how threats and coping appraisals, as constructs from protection motivation theory, influence the implementation of telehealth services. The empirical results after data collection and analysis from 543 respondents' using structural equation modelling technique showed that perceived patients' information security threat and privacy risk, perceived telehealth systems security threat and self-efficacy had a significant effect on health professionals' behaviours to use telehealth services. Health professionals' behaviour also had a significant effect on actual telehealth service use. Response efficacy however had no significant effect on health professionals' adoption of telehealth services. The study results contribute to empirical knowledge by identifying health professionals' preparedness to use telehealth services.

Keywords: telehealth services; patient information; security threats; privacy risk; healthcare professionals.

Reference to this paper should be made as follows: Kissi, J., Dai, B., Achmpong, E.K., Dankyi, A.B. and Antwi, J. (2023) 'An empirical study of healthcare professionals' willingness to utilise telehealth services based on protection motivation theory', *Int. J. Healthcare Technology and Management*, Vol. 20, No. 1, pp.74–89.

Biographical notes: Jonathan Kissi is a Lecturer at the Department of Health Information Management, School of Allied Health Sciences, University of Cape Coast – Ghana. His research interests include electronic health records, telehealth services, ICT in healthcare services and management information systems.

Baozhen Dai is a PhD Supervisor at the School of Management, Jiangsu University – China. Her major research field and interests are focused on health policy and management, old age health security and health insurance reform.

Emmanuel Kusi Achmpong is a Senior Lecturer at the Department of Medical Education and Information Technology (DMEIT), School of Medical Sciences, University of Cape Coast – Ghana. His research interests include electronic health records, health informatics, cloud computing security, and ICT in medical education.

Alex Boadi Dankyi is a Research Fellow at the Directorate of Research, Innovation and Consultancy, University of Cape Coast – Ghana. His research interests include human capacity development, human resource management, quality of health services andorganisational innovations.

Joseph Antwi is a Principal Administrator at the Department of Health Information Management, University of Cape Coast – Ghana. His research interests are in the area of health services administration and human resource management.

1 Introduction

As stated by the World Health Organization (WHO), social determinants of health factors are factors outside the healthcare organisational settings that substantially impact the operations of healthcare activities (WHO, 1998; Peredina and Allen, 1994). These determinants may include social, technological, regulatory, and political factors. Nevertheless, this current study concentrates on some technological aspects outside the healthcare setting that impedes health professionals' motivation to accept and use telehealth services. Previous health information research has attempted to identify why healthcare professionals are threatened by technological factors influencing their acceptance of healthcare systems. However, understanding such determinants of technological systems in health is a topic of ongoing interest (Straub and Welke, 1998; Lee and Kozar, 2005).

Predominant information systems acceptance theories, including the theory of planned behaviour, innovation diffusion theory, and technology acceptance model (TAM), are often used as theoretical frameworks to address the acceptance of technological innovations in other disciplines. These theories can address determinants influencing technological acceptance in healthcare systems adoption (Straub and Welke, 1998; Lee and Kozar, 2005). To examine these determinant factors within the confines of healthcare, various models have been proposed. The researchers adopted the protection motivation theory (PMT) in this present study. The theory gives a clear view of the healthcare environment and technological determinants that can daunt the successful implementation of technological innovation in the healthcare industry. To sustain such a competitive situation, the healthcare systems adapt to the changing and uncertain technological conditions (Rogers, 1983; Block, 1998).

PMT theoretical framework was adopted because its application has effectively predicted and understood the varied array of preventive actions (Milne et al., 2000). This current research expands the original PMT model by adding 'individual behavioural intentions' and 'actual systems use' from the TAM to 'perceived patient's information security', 'perceived patient's information privacy', 'perceived telehealth systems security', 'self-efficacy' and 'response efficacy' as threats and coping appraisals. These factors are determinants outside the confines of the healthcare institution that causes significant problems in the successful implementation of telehealth services.

1.1 Telehealth services adoption

Telehealth integrates information and telecommunication technologies with medicine. The concept is realised by assisting the daily activities of healthcare professionals in diagnosis, treatment, and consultations in patient care delivery (WHO, 1998; Bashshur et al., 2005). The approach broadens the patient care service to a large segment of hard-to-reach areas, especially in developing countries. Telehealth service provides a means to enhance access to quality healthcare for inhabitants in marginalised societies and minimises the brain drain of skilled medical professionals' shortages (WHO, 1998; Bashshur et al., 2005). Despite the bright benefit and opportunities for telehealth services, its adoption and use has been problematic in some places, and its successful implementation still hangs in the balance. Several studies have investigated the reason

behind the slow telehealth adoption. They have attributed it to factors like lack of policies regarding its operations, lack of patient information security and privacy standards, and healthcare professionals' fear of threats with the system that breaches their professional ethics in treating patients. However, other studies have shown that there have been inadequate or fewer discussions on the invasions of threats and coping appraisals in telehealth services (WHO, 1998; Bashshur et al., 2005; Mairinger et al., 1998),(Scott and Varghese, 2004).

Several researchers divulge that the demands in telecommunication technologies by healthcare organisations all over the world have grown significantly due the current pandemic like COVID-19. Technology acceptance standards in healthcare have become critical with management and implementation issues. Many telehealth applications are being developed to boost patient care delivery in this pandemic era (WHO, 1998; Bashshur et al., 2005). The use of the internet, which champions telehealth services applications, raises issues with 'perceived patient information security threats', 'perceived patient information privacy risk', 'perceived threats in systems integrations', 'health professionals' self-efficacy', and 'health professional response efficacy'. The most predominant threats that usually occur in telehealth services include; privacy risk, which involves lack of controls on the disclosure, collection, and use of sensitive patient information. Other security threats deal with the breach of confidentiality during the collection and transmission of sensitive data, unauthorised contact to the functionality of stored data or backup devices, and untrusted circulation of hardware and software to patients (Hale and Kvedar, 2014; Hall and Mcgraw, 2014).

Numerous research efforts are being carried out to identify the factors that will motivate healthcare professionals to utilise telehealth services. Other studies also propose vigorous security policy enforcement and plans as a response measure. These researches will encourage health professionals to use telehealth programs without fear of privacy risks and security threats (Zhao and Pechmann, 2007; Cody et al., 2008). In clinical settings, few studies have investigated the individual behavioural intents that efficiently persuade healthcare professionals' adoption of security threats and privacy risks. Most behavioural research concentrates on standard information system models and only examines the efficiency factors (Ease-of-use) and effectiveness (relative advantage) without discussing the threat and risk factors. This present study investigates health professionals' zeal to utilise telehealth services based on the constructs of threats and coping appraisals deducted from the PMT.

2 Theoretical background

2.1 Protection motivation theory

Many theories have been proposed to investigate health-related behavioural changes in healthcare settings. PMT integrates the role of health-related information in effecting behavioural changes (Rogers, 1983; Block, 1998). PMT foundation in healthcare sciences motivates healthcare professionals to evade unhealthy behaviour through fear. This fear usually happens when threatened with health information threats and privacy or distorted clinical information in distributed systems (Webb et al., 2010). According to PMT,

viewing health-related data from a location provides the momentum for the healthcare personnel to assess the severity and probability of an event occurrence, belief's in the effectiveness of the suggestion offered in the message or information. Lastly, the health personnel can give tips on the received messages (Block, 1998). PMT theory is divided into two parts: coping and threat appraisals. A coping appraisal comprises response efficacy and self-efficacy (Tunner et al., 1989; Rogers and Mewborn, 1976). Threat appraisal examines the dangers or risks factors that may decrease or increase the chances of making a maladaptive response. It also refers to health professionals' subjective decisions on the risk of other security and privacy breaches on patients' information or antisocial behaviours. These threats of privacy daunt the smooth functioning of telehealth service (Tunner et al., 1989; Rogers and Mewborn, 1976).

2.2 Hypotheses development

In telehealth services adoption, health professionals use threat appraisals to protect themselves from perceived threats or risks. Threat appraisal influences various health professionals' attitudes and behavioural reactions. Although there are individual differences, health professionals are sometimes at risk for using a telehealth service due to threat invasion and at times unwilling to participate in telehealth services. If health professionals feel more threatened regarding the consequences of adapting to security threats or privacy risks, it deters their behavioural intentions, which intimidates telehealth utilisation among such professionals. In telehealth services, several clinical applications and systems come into play by connecting applications of different services and methods between the initiating and receiving facilities. These are championed by adaptive network services used in the health facilities and expose the service to several perceived threats (Prentice-Dunn and Rogers, 1986). Threats may occur due to breaches to the patients' information (security or privacy) and lack of oversight responsibilities in the distributed systems security integration protocols. The healthcare professional's confidence in the telehealth services protocols to prevent unauthorised users from invading the telehealth services and intercepting the service data, videos, or images boosts their intent to utilise it (Block, 1998; Prentice-Dunn and Rogers, 1986). A health professional may be intimidated by the perceived security and perceived privacy breaches that may take place in health information management systems through network interoperability or data dissemination from one location to the other. The health professional may also be threatened by the potential consequences of distorted clinical information in actual telehealth service delivery (Plotnikoff et al., 2009). Given these elucidations, we might expect health professionals utilise the telehealth service if they have an improved understanding of its security threats and privacy risks, and the service usage will be easy, resulting in quality health outcomes. Based on the above discussion, we hypotheses that:

H1: Perceived patients' information security threat (PASEC) influences health professional's behaviours to use telehealth services.

H2: Perceived patients' information privacy risk (PAPRIV) impacts health professional's behaviours to use telehealth services.

H3: Perceived telehealth systems security threat (TEMSEC) influences health professionals' behaviours to use telehealth services.

Coping appraisals about telehealth services adoption consist of self-efficacy, which is the confidence of a healthcare professional to use telehealth services successfully without any fear. Response efficacy is the healthcare professional's assurance in the telehealth system protocols to prevent hackers from invading telehealth services and not intercepting telehealth data, videos or images (Block, 1998; Prentice-Dunn and Rogers, 1986). Based on this, we hypothesise that:

H4: Self-efficacy (SELEFF) significantly impacts health professionals' adoption of telehealth services.

H5: Response efficacy (RESPEFF) significantly influences health professionals' adoption of telehealth services.

H6: Health professionals' behaviour (INDINT) is positively related to actual telehealth service use (ACTUSE).

3 Method

3.1 Settings

This study was conducted in Ghana, a Sub-Saharan country in West Africa, between September 2018 and April 2019. The country presently has 16 regions. The study was conducted in the Eastern part with about 19,323 km^2 land size and the third inhabited province. Population growth in the Eastern region has brought about new technological innovations in healthcare facilities. The research was steered in the area due to the innovations in its health service delivery, shortage of health professionals, infrastructural deficiencies, difficulties in service delivery and demands for quality in healthcare delivery (Ghana Health Service Annual Report, 2017; Ekanoye et al., 2017). This economic predicament pushes healthcare authorities to utilise telehealth services in clinical operations. The researchers were inspired by the healthcare indicators and asked the Eastern Regional Health Directorate Ethical Review Committee to research the consequences of threats and coping appraisal on telehealth services in the region. Informed consent was sent to the Administrators of the hospitals where the study was carried out. To fulfil the standards and achieve the research purpose, a purposive and convenience sampling technique was applied to choose participants from four health institutions: Holy Family Hospital, Eastern Regional Hospital, Kwahu Government Hospital, and the Regional Health Directorate. These hospitals were selected due to telehealth activities' utilisation, presence and management. The telehealth services used in the selected facilities were teleconsultation services for hypertension education, diabetics education, antenatal education and minor surgical services. The Eastern Regional Hospital was the referral station for telehealth activities in the catchment area. Health Professionals who patronised these telehealth services were rarely motivated and trained by their hospital management.

3.2 Study design, participants and sampling

Questionnaires were developed for the study based on extant literature (Craig and Patterson, 2005; Olver and Selva-Nayagam, 2000; Creswell, 2007; Kline, 2005;

Fornell and Larcker, 1981) with necessary wording changes and validation customised to telehealth services and the target profession. Physicians, Physician Assistants, Nurses, Healthcare Administrators, and Telehealth Service Providers were deliberately chosen considering their experiences, job roles, job knowledge, and job plans in telehealth services. They were better placed to answer numerous questions. The research took place in the out-patient departments, emergency care units, maternity wards, in-patient departments, paediatrics departments and surgical departments because these departments of the hospitals regularly utilise the telehealth services.

A questionnaire encompassing the constructs PASEC (5 items), PAPRIV (3 items), TEMSEC (4 items), SELEFF (4 items), RESPEFF (3 items), INDINT (4 items) and ACTUSE (4 items) was developed by the researchers with a five-point Likert scale to evaluate the answers ranging from 5- strongly agree to 1- strongly disagree and disseminated to the qualified staff in both soft and hard copy forms. The questionnaire was addressed directly to participants who were voluntarily present to answer the questions. Participants who had busy schedules and could not attend to the researchers immediately due to their job plans gave out their phone contacts and softcopies were sent to them to complete at their opportuneness. Participants were contacted every two weeks using short messages systems and emails as a tracking approach because it was tough to connect to individual participants. The questionnaire asked for participants' opinions on managing threats and coping appraisals in using telehealth services in their professional tasks. Out of 625 questionnaires distributed, 612 were recovered from participants after the data gathering process. 69 responses were exempted due to insufficiencies in answers. Finally, the data analysis of this study was based on 543 respondents' responses representing 78.6%.

4 Analysis and results

To check if the measurement and structural models depict the standards for evidence-based study, AMOS (v.23) and SPSS (v.23) were utilised in structural equation modelling (SEM) approach. All variables in the model were chosen from the questionnaires used in the data gathering process. These constructs are represented (Tables 1–4).

4.1 Demographics of respondents

This study's respondents comprise of 43.6% Nurses, 7.9% Physicians, 27.8% Physician Assistants, 8.5% Healthcare Administrators, and 12.2% Telehealth Service Providers. Respondents between ages 31 and 40 were in the majority (45.5%). 82.9% of the respondents were university degree holders, and the most common and the least qualified were Ordinary level certificate holders representing 7.2%.

Table 1 Measurements and confirmatory factory analysis

Construct	*Items*	*Unstandardised estimate*	*Standard error*	*Critical ratio*	*Standardised factor loadings*	*p-value*	*Average variance extracted*	*Construct reliability*	*Cronbach's alpha*
PASEC	PASEC1	1.000	–	–	0.902				
	PASEC2	0.972	0.031	31.355	0.890	***			
	PASEC3	1.011	0.034	29.735	0.876	***	0.736	0.933	0.932
	PASEC4	0.948	0.032	29.625	0.862	***			
	PASEC5	1.158	0.032	36.188	0.752	***			
PAPRIV	PAPRIV1	1.000	–	–	0.875				
	PAPRIV2	1.093	0.043	25.419	0.868	***	0.760	0.904	0.903
	PAPRIV3	1.020	0.040	25.500	0.871	***			
TEMSEC	TEMSEC1	1.000	–	–	0.885				
	TEMSEC2	1.081	0.046	23.500	0.817	***			
	TEMSEC3	1.114	0.048	23.208	0.807	***	0.687	0.897	0.895
	TEMSEC4	0.964	0.041	23.512	0.807	***			
SELFEFF	SELEFF1	1.000	–	–	0.885				
	SELEFF2	1.091	0.040	27.275	0.880	***			
	SELEFF3	0.990	0.048	20.625	0.786	***	0.703	0.904	0.902
	SELEFF4	0.985	0.041	24.024	0.799	***			

Table 1 Measurements and confirmatory factory analysis (continued)

Construct	*Items*	*Unstandardised estimate*	*Standard error*	*Critical ratio*	*Standardised factor loadings*	*p-value*	*Average variance extracted*	*Construct reliability*	*Cronbach's alpha*
RESPEFF	RESPEFF1	1.000	–	–	0.759				
	RESPEFF2	0.862	0.072	11.972	0.716	***	0.510	0.757	0.756
	RESPEFF3	0.828	0.07	11.829	0.665	***			
INDINT	INDINT1	1.000	–	–	0.651				
	INDINT2	1.230	0.074	16.622	0.839	***			
	INDINT3	1.336	0.076	17.579	0.934	***	0.653	0.881	0.874
	INDINT4	1.108	0.071	15.606	0.783	***			
ACTUSE	ACTUSE1	1.000	–	–	0.928				
	ACTUSE2	0.878	0.041	21.415	0.782	***			
	ACTUSE3	0.794	0.044	18.045	0.694	***	0.603	0.856	0.845
	ACTUSE4	0.902	0.052	17.346	0.674	***			

PASEC: Perceived patient security, PAPRIV: Perceived patient privacy, TEMSEC: Perceived telemedicine systems security, SELEFF: Self efficacy, RESPEFF: Response efficacy, INDINT: Individual behavioral intentions; ACTUSE: Actual telemedicine use.

***$p < 0.001$.

4.2 Measurement of confirmatory factor analysis

Measurement items were assessed based on reliability and validity, and constructs exceeding their desired limit were utilised. As recommended by scores of researchers, we operationalised threats and coping appraisals among healthcare professionals as the reflective variables. The measurement constructs were appraised based on discriminant validity, which presents the items self-determine; convergent validity shows the items associations with their appropriate constructs and constructs reliability, which specifies the consistency of the measurement items (Kline, 2005; Fornell and Larcker, 1981; Byrne, 2010). From the theoretical basics of the above procedures, all items were meaningfully investigated. The distinct constructs Cronbach's alpha values of 0.932 to 0.756 were higher than the scale of 0.70. The convergent validity was calculated, and the average variance extracted (AVE) for all reflective constructs was increased than the desired mark of 0.5, from 0.760 to 0.510.

Table 1 depicts the measurements and confirmatory factor investigation.

A confirmatory factor analysis (CFA) was utilised to assess the measurement models for the reliability and validity constructs. In this research, eight measures were used to determine the goodness of fit of the CFA (Fornell and Larcker, 1981; Byrne, 2010; Hair et al., 2010). All the variables reached the recommended values signifying that the model was suitable for assessment. Table 2 depicts the fitness of the study model.

Table 2 Overall fit of the research model

Model-fit index	*Recommended value*	*Score*
Chi-square/degree of freedom (X^2/df)	≤3.00	1.294
Goodness-of-fit index (GFI)	≥0.90	0.948
Adjusted goodness-of-fit index (AGFI)	≥0.90	0.938
Non-normed fit index (NNFI)	≥0.90	0.954
Comparative fit index (CFI)	≥0.90	0.989
Root mean square residual (RMR)	≤0.08	0.049
Tucker-Lewis index (TLI)	≥0.90	0.988
Root mean square error of approximation (RMSEA)	≤0.08	0.023

Table 3 Discriminant validity

ITEM	*PASEC*	*PAPRIV*	*TEMSEC*	*SELFEF*	*RESPEFF*	*INDINT*	*ACTUSE*
PASEC	**0.858**						
PAPRIV	0.613**	**0.872**					
TEMSEC	0.609**	0.623**	**0.829**				
SELFEF	0.568*	0.663**	0.553*	**0.838**			
RESPEFF	0.523*	0.511*	0.521*	0.512*	**0.714**		
INDINT	0.644**	0.634**	0.602**	0.618**	–0.428	**0.808**	
ACTUSE	0.682***	0.671***	0.623**	0.653***	–0.532	0.615**	**0.777**

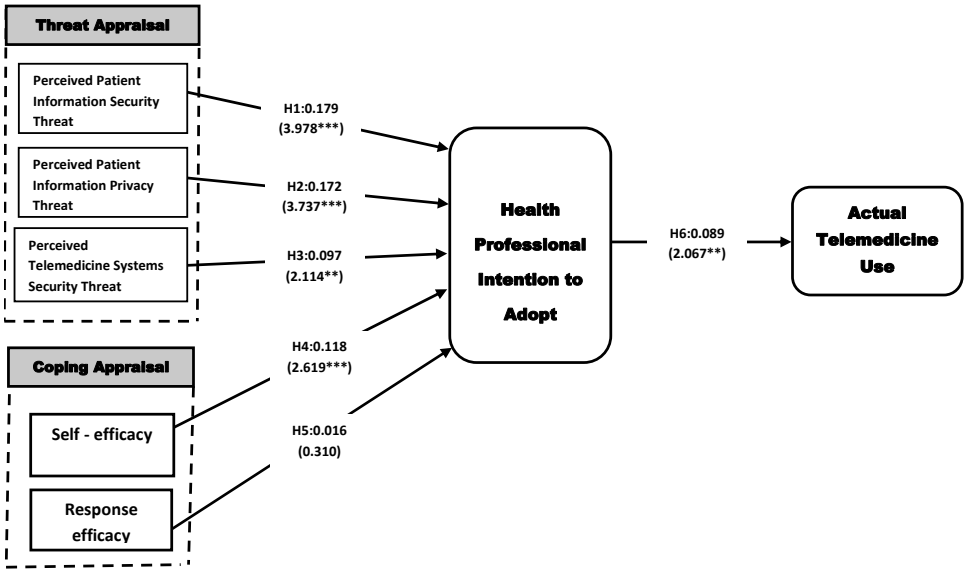
* ≈ P-value significant at 5% (0.05); ** ≈ P-value significant at 1% (0.01); *** ≈ P-value significant at 0.1% (0.001); √AVE is bold and underlined.

The discriminant validity was estimated using the square root of AVE to substitute for the correlation coefficient matrix diagonals, with higher figures linking the correlation coefficients. This depicts that reflective constructs are different from each other. The measures in the research emphasised an acceptable confirmation of convergent and discriminant validities, and uni-dimensionality for the structural model (Fornell and Larcker, 1981; Byrne, 2010; Hair et al., 2010). Table 3 illustrates discriminant validity.

4.3 Hypothesis testing

Table 2 summarises the structural model fit as evaluated using goodness-of-fit measures. The values were within recommended limits. In Table 3, five were positively supported out of the six assumptions made, and one was rejected. The structural path diagram in Figure 1 depicts the significant associations of all assumptions made but at different significant levels. The constructs in the model have empirical backings from other research studies.

Figure 1 The causal path diagram depicts the associations between constructs



*t0.05 = 1.960, **t0.01 = 2.576, ***t0.001 = 3.29.

Hypothesis 1, PASEC, suggested a significant effect on behavioural intention to use telehealth services. The study confirmed a positive association in affirming the assumptions ($\beta = 0.179$, $p < 0.001$). The findings are in tandem with similar works (Hale and Kvedar, 2014; Whitman and Mattord, 2008; Angst and Agarwal, 2009; Lee and Larsen, 2009) showed in telehealth services.

In hypothesis 2, the health professionals' behavioural intention was positively affected by PAPRIV, affirming the assumptions ($\beta = 0.172$, $p < 0.001$). Our study findings are in tandem with similar works (Hall and Mcgraw, 2014; Whitman and Mattord, 2008; Angst and Agarwal, 2009; Lee and Larsen, 2009).

In hypothesis 3, the study results were statistically positive, confirming the stated assumptions with beta values of 0.097 ($p < 0.05$). The study result is similar to studies of Hale and Kvedar (2014), Hall and Mcgraw (2014), Whitman and Mattord (2008), Angst and Agarwal (2009), and Lee and Larsen (2009).

Our results endorse the study hypothesis 4 made as positive ($\beta = 0.118$, $p < 0.01$) but with hypothesis 5, the study findings surprisingly did not support the stated idea; this is contrary to the results of several studies (Lee and Larsen, 2009; Bandura, 1977).

Finally, with hypothesis 6, health professionals' behavioural intention significantly impacted the real telehealth services utilisations with a beta value of 0.089 ($p < 0.05$). The findings are in tandem with the works (Craig and Patterson, 2005; Lee and Larsen, 2009; Bandura, 1977).

The empirical results of the stated assumptions are seen in Table 4.

Table 4 Hypothesis testing

Hypothesis	*Path*	*Unstandardised estimate*	*Standard error*	*Critical ratio* (C.R.,t)	*Standard estimate*	*p-value*	*Findings*
H1	PASEC → INDINT	0.183	0.046	3.978	0.179	***	Supported
H2	PAPRIV → INDINT	0.142	0.038	3.737	0.172	***	Supported
H3	TEMSEC → INDINT	0.093	0.044	2.114	0.097	*	Supported
H4	SELFEFF → INDINT	0.110	0.042	2.619	0.118	**	Supported
H5	RESPEFF → INDINT	0.018	0.058	0.310	0.016	0.755	n/s
H6	INDINT → ACTUSE	0.093	0.045	2.067	0.089	*	Supported

*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$.

5 Discussions and implications

To determine telehealth services' success in society, one must identify the threats and coping appraisals and ascertain how they collectively affect its successful implementation. This was to be achieved with Rogers' (Rogers, 1983; Block, 1998) PMT. The overall outcome of this study indicates that all selected constructs were appropriate for examining threats and coping appraisals among health professionals. The model provided solid empirical support from other kinds of literature and was also evaluated by the analysis of the study. Judged by path coefficients and the confirmatory factor analysis, PMT has strong macro indicators that encourage the effective implementation of telehealth services in society (see Table 1).

At present, several studies reviewed indicated that few types of research had been conducted on threats and coping appraisals of telehealth services in Ghana. However, following the poor ratio of health professionals to patients leading to the adoption of telehealth services as indicated in reports by the Ghana health services, it is essential to

appreciate the threats and coping appraisals that intimidate the full utilisation of telehealth services. This present research proves that the adoption of telehealth has been dramatically affected by 'perceived patients' information security threats', 'perceived patients' privacy risk', 'perceived telehealth system security threat', 'health professionals' self-efficacy', and 'individual behavioural intentions to use telehealth service' (see Table 4). This means that the development of rigorous security systems for patient health information and systems security is paramount in telehealth services. Human and non-human agents' causes of threats in telehealth services must be assessed to prevent unauthorised users. These include hackers, intruders, and denial of service from modifying, intercepting, and editing vital patient information, images, videos, or breaking into the telehealth system network connectivity. Some non-human agents that need to be considered when telehealth services may also include floods, fire outbreaks, lightning, hurricanes, earthquakes, etc. (Kissi et al., 2018a). Kissi et al. (2018b) have given some measures that ought to be considered to alleviate such threats. For health professionals to be convinced with the deployment of secure applications, internet, and intranet infrastructures, strong cautions should be emphasised on the security controls when developing telehealth services.

Again, the study results have shown that health professionals use telehealth services. However, they are worried about their patient's health information, especially with security threats and privacy risk issues. California HealthCare Foundation (2010) conducted a similar study to ascertain adults' interest in telehealth systems. The study had a response rate of 66% participation. The results revealed that almost half of the participants were interested in telehealth services. However, the participants believed that there were issues relating to the privacy of their personal medical information and need to be addressed while still emphasising that telehealth services will improve their healthcare (California HealthCare Foundation, 2010; Walker et al., 2009).

Studies by other researchers have also shown that people are ready to welcome privacy risks when they perceive that the risk of sharing health information in using telehealth services is lower than the health benefits they may obtain. A similar study was conducted by Vodicka et al. (2013) where participants with chronic conditions were interested in how the telehealth service can help improve their health outcomes. In contrast, the other healthy participants were concerned with the privacy risk in health technology systems.

Another caveat to this study is that health professionals should confidently trust their telehealth service before they put it to practice despite the potential benefit of telehealth services. This will boost their professional self-efficacy (see Table 4), and their patients will also have confidence in such systems. This plays an imperative role in patients' adoption of telehealth services. Patients' trust in their health professionals and telehealth services will contribute to the continuity of care and improved treatment adherence by demonstrating good patient-physician communication.

Finally, as part of confidentiality issues, health professionals need to be abreast with the health institutions' telehealth services security and privacy regulation and discuss same with their patients as part of their ethical obligation to ensure patient confidentiality. They are also to discuss the benefits, threats, and risks associated with telehealth services with their patients as a way of familiarising them with their patient-centred care plan.

6 Limitations of the study

Although the results of this research are promising, there are certain limitations on their promotion. First, the data gathering process was subject to questionnaire management. It is necessary to conduct several studies using different data collection methods to generalise the results. Second, the research did not stress precise telehealth services but emphasised a specific category of specialists in specialised hospitals. The thinking styles of these people can be prejudiced by accurate public health systems and regional features. Third, the data-gathering cycle was short, which led to low involvement. Healthcare administrators need to be very careful when maximising results. Further research should gather information from a wide range of respondents and large respondents.

7 Conclusion

Ghana's healthcare sector is working tirelessly to ensure that telehealth services are espoused and utilised in several hospitals. This service will assist in bridging the barriers among patients and healthcare professionals, more importantly, in clinical care management, where specialist medical interventions are required. This research is paramount because the Ministry of Health calls for the commercialisation of numerous telehealth centres. Threats and coping appraisals, which form part of the significant telecommunication determinants factors in telehealth services, must be carefully evaluated. To address this critical issue, this study applied the protection motivation theory to examine how the existing PMT variables and new threats appraisals can influence health professionals' intentions to adopt telehealth services using data collected from healthcare professionals.

PMT is widely used in understanding privacy and security intent in different contexts. However, there have been significant differences in other PMT variables' impact on security intents. Concerns about the privacy and security of telehealth services may harmfully affect health professionals' trust in the service. This will subsequently intimidate the improvements in effectiveness, usefulness, and accessibility to service deliveries. The current widespread and use of telehealth services in patients-health associations may require that comprehensive protocols and standards operating policies be part of telehealth applications to ensure robust security and privacy threats appraisals.

Regarding coping appraisal dimensions, self-efficacy significantly impacted an individual's intention to adopt and use telehealth services. This implies that Health professionals must be confident about the decisions and judgements using telehealth services. Health professionals can also aid telehealth services to succeed by creating patient-centred care programs that efficiently utilises telehealth tools. In addition, before telehealth implementations, it's essential to establish threats and cope with appraisals protocols for all participating institutions.

Finally, future research may incorporate health professionals' responsibilities and safety habit strength as coping appraisals, which have been established in other works of literature to be strong predictors of security intentions.

References

Angst, C. and Agarwal, R. (2009) 'Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion', *MIS Quarterly*, Vol. 33, No. 2, pp.339–370.

Bandura, A. (1977) 'Self efficacy: toward a unifying theory of behavioral change', *Psychological Review*, Vol. 84, pp.191–215.

Bashshur, R., Shannon, G. and Sapci, H. (2005) 'Telemedicine evaluation', *Telemedicine Journal and e-Health*, Vol. 1, No. 3, pp.296–316.

Block, L.G. (1998) *Beyond Protection Motivation: An Integrative Theory of Health Appeals*, pp.1584–1608.

Byrne, B.M. (2010) *Structural Equation Modeling With AMOS: Basic Concepts*, Applications, and Programming, 2nd ed., Routledge, New York.

California HealthCare Foundation (2010) *Consumers and Health Information Technology: A National Survey*, California HealthCare Foundation, Oakland CA.

Cody, E., Sharman, R., Rao, R.H. and Upadhyaya, S. (2008) 'Security in grid computing: a review and synthesis', *Decision Support Systems*, Vol. 44, No. 4, pp.749–764.

Craig, J. and Patterson, V. (2005) 'Introduction to the practice of telemedicine', *Journal of Telemedicine and Telecare*, Vol. 11, No. 1, pp.3–9.

Creswell, J.W. (2007) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 2nd ed., Sage, Thousand Oaks, CA.

Ekanoye, F., Ayeni, F., Olokunde, T., Mende, C.M., Nina, V. and Mbarika, V. (2017) 'Telemedicine diffusion in a developing country: a case of Ghana', *Science Journal of Public Health*, Vol. 5, No. 5, pp.383–387.

Fornell, C. and Larcker, F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error', *J. Marketing Res*., pp.39–50.

Ghana Health Service Annual Report (2017) https://www.Ghanahealthservice.org (Accessed 30 June, 2019).

Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2010) *Multivariate Data Analysis*, 7th ed., Prentice Hall, Upper Saddle River, NJ.

Hale, T.M. and Kvedar, J.C. (2014) 'Privacy and security concerns in telehealth', *Virtual Mentor*, Vol. 16, No. 12, pp.981–985, https://doi.org/10.1001/virtualmentor.2014.16.12.jdsc1-1412

Hall, J.L. and Mcgraw, D., (2014) 'For telehealth to succeed, privacy and security risks must be identified and addressed', *Health Affairs*, Vol. 33, No. 2, pp.216–221, https://doi.org/10.1377/hlthaff.2013.0997

Kissi, J., Dai, B., Owusu-marfo, J., Asare, I., Opuni, M. and Benedicta Clemency, A.A. (2018a) 'A review of information security policies and procedures for healthcare services', *Canadian J. of App Sci.*, Vol. 6, No. 2, pp.812–819.

Kissi, J., Dai, B., Lemency, B.A. and Amoah-anomah, G. (2018b) 'Reliance on cryptography of cloud computing in healthcare information management, lessons for Ghana health service', *Int. J. Inform. Sec. Sci.*, Vol. 7, No. 3, pp.111–125.

Kline, R.B. (2005) *Principles and Practice of Structural Equation Modeling*, 2nd ed., The Guilford Press, New York.

Lee, Y. and Kozar, K. (2005) 'Investigating factors affecting the adoption of anti-spyware systems', *Communications of the ACM*, Vol. 48, No. 3, pp.72–78.

Lee, Y. and Larsen, K.R. (2009) 'Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software', *European Journal of Information Systems*, Vol. 18, No. 2, pp.177–187, https://doi.org/10.1057/ejis.2009.11

Mairinger, T., Netzer, T.T., Schoner, W. and Gschwendtner, A. (1998) 'Pathologists' attitudes to implementing telepathology', *Journal of Telemedicine and Telecare*, Vol. 4, No. 1, pp.41–46.

Milne, S., Sheeran, P. and Orbell, S. (2000) 'Prediction and intervention in health-related behavior: a meta-analytic of protection motivation theory', *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp.106–143.

Olver, I.N. and Selva-Nayagam, S. (2000) 'Evaluation of a telemedicine link between darwin and Adelaide to facilitate cancer management', *Telemed. J.*, Vol. 6, No. 2, pp.213–218.

Peredina, D.A. and Allen, A. (1994) 'Telemedicine technology and clinical applications', *Journal of the American Medical Association*, Vol. 2, No. 73, pp.483–488.

Plotnikoff, R.C., Rhodes, R.E. and Trinh, L. (2009) 'Protection motivation theory and physical activity: a longitudinal test among a representative population sample of Canadian adults', *J. Health Psychol.*, Vol. 14, No. 8, pp.1119–34, https://doi.org/10.1177/1359105309342301

Prentice-Dunn, S. and Rogers, R.W. (1986) 'Protection motivation theory and preventive health: beyond the health belief model', *Health Education Research*, Vol. 1, No. 3, pp.153–161.

Rogers, R.W. (1983) 'Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation', in Cacioppo, J.T. and Petty, R.E. (Eds.): *Social Psychophysiology*, Guilford, New York, NY.

Rogers, R.W. and Mewborn, R.C. (1976) 'Fear appeals and attitude change: effects of a threat's noxiousness, probability of occurrence, and the efficacy of coping responses', *Journal of Personality and Social Psychology*, Vol. 34, pp.54–61.

Scott, R. and Varghese, S. (2004) 'Categorizing the telehealth policy response of countries and their implications for complementarity of telehealth policy', *Telemedicine Journal and e-Health*, Vol. 10, No. 1, pp.61–69.

Straub, D.W. and Welke, R.J. (1998) 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, Vol. 22, No. 4, pp.441–465.

Tunner Jr., J.F., Day, E. and Crask, M.R. (1989) 'Protection motivation theory: an extension of fear appeals theory in communication', *Journal of Business Research*, Vol. 19, No. 4, pp.267–276.

Vodicka, E., Mejilla, R., Leveille, S.G., Ralston, J.D., Darer, J.D., Delbanco, T., … and Elmore, J.G. (2013) 'Online access to doctors' notes: patient concerns about privacy', *J. Med Internet Res.*, Vol. 15, No. 9, p.e208.

Walker, J., Ahern, D.K., Le, L.X. and Delbanco, T. (2009) 'Insights for internists: 'I want the computer to know who I am', *J. Gen Intern Med.*, Vol. 24, No. 6, pp.727–732.

Webb, T.L., Sniehotta, F.F. and Michie, S. (2010) 'Using theories of behaviour change to inform interventions for addictive behaviours', *Addiction*, Vol. 105, No. 11, pp.1879–1892, https://doi.org/10.1111/j.1360-0443.2010.03028.x

Whitman, M.E. and Mattord, H.J. (2008) *Management of Information Security*, 2nd ed., Thomson Course Technology, Boston, Massachusetts.

WHO (1998) *A Health Telematics Policy in Support of WHO's Health-For-All Strategy for Global Health Development: Report of the WHO Group Consultation on Health Telematics*, 11–16 December, Geneva, 1997, World Health Organization, Geneva.

Zhao, G. and Pechmann, C. (2007) 'The impact of regulatory focus on adolescents' response to anti smoking advertising campaigns', *Journal of Marketing Research*, Vol. XLIV, pp.671–687.