Culture Matters: Factors Affecting the Adoption of Telemmedicine

Parand Mansouri-Rad  
University of Texas at El Paso  
pmansourirad@utep.edu

M. Adam Mahmood  
University of Texas at El Paso  
mahmood@utep.edu

Sharon E. Thompson  
University of Texas at El Paso  
sthompson@utep.edu

Karl Putnam  
University of Texas at El Paso  
kputnam@utep.edu

Abstract

The present research investigates the influence of culture on telemedicine adoption and patient information privacy, security, and policy. The results, based on the SEM analysis of the data collected in the United States, demonstrate that culture plays a significant role in telemedicine adoption. The results further show that culture also indirectly influences telemedicine adoption through information security, information privacy, and information policy. Our empirical results further indicate that information security, privacy, and policy impact telemedicine adoption.

1. Introduction

In the past, simple devices such as flags, signs, and bells were commonly used to communicate the presence of diseases [14]. Recently, a new model of communicating health information and providing healthcare has emerged which blends the delivery of medicine with information and telecommunication technologies (ICT). An ongoing and increasing demand for healthcare services is accentuated by an acute shortage of healthcare professionals and hospital facilities especially in rural areas. The development of this new model of distance healthcare, also known as telemedicine, has increased significantly over the last few years as manifested by a fast growing number of programs [38]. Telemedicine is using information technologies to transfer information and provide health care services across geographical barriers [52]. Analysts of the Report Buyer, the online destination for business intelligence, forecasts that the telemedicine service market is expected to grow from $3.6 billion in 2007 to $8.3 billion in 2012.

Despite this bright future for telemedicine, its adoption has been problematic. Many studies investigate the reason behind this slow adoption. Adam (2001) and Bashur, Shanon, and Spaci [2005] [1, 7], for example, blame the lack of availability of information and telecommunication technologies (ICT) for this lack of adoption. Anderson (2000) and Scott and Vargese (2004) [3 and 42] blame it on regulation obstacles. Hu, Chau, and Sheng (2000) and Kiffle, Mbarika, and Payton (2005) cite human factors [24, 29]. Others see cultural barriers as a problem in adopting telemedicine [24, 45, 6]. Most studies concentrate on the impact of ICT factors on adopting telemedicine [1, 7]. Hu et al. (2000) and Kiffle, Mbarika, and Brandy (2006) report human and cultural factors have more effect on telemedicine especially in developed countries such as U.S. and UK [24, 30]. Ilie, Courtney and Van Slyke (2007) investigated such human factors on U.S. physicians’ acceptance of Electronic Medical Records (EMR) [26]. They found that U.S. physicians showed negative attitudes toward the EMR and viewed it as difficult to navigate [26]. Telemedicine and EMR are related concepts. In order to have telemedicine, it is necessary for there to be EMR to transmit between telemedicine locations, so the concerns for adoption of both EMR and telemedicine should be similar.


Previous studies in the area, such as the aforementioned discussion, are not thorough in investigating the lack of telemedicine adoption. Most of these studies are limited in scope and focused only on one antecedent. As such these studies did not provide an in-depth analysis of the adoption of
telemedicine. The objective of the present research is to conduct a comprehensive research study that rigorously evaluates the effect of culture on telemedicine adoption and patient information privacy, security, and policy. The research questions are: Does culture play a direct role in telemedicine adoption? Does culture play an indirect role through information security, privacy, and policy in telemedicine adoption? Do information security, privacy, and policy play direct roles in telemedicine adoption? In the next section we provide the literature review.

2. Literature Review

Previous research on telemedicine adoption, as stated earlier, is limited in scope. While these studies have expanded the understanding of telemedicine adoption from various perspectives, only a few research studies considered culture as a construct. No studies have provided a comprehensive evaluation on the implementation and adoption of telemedicine. The present research seeks to focus on constructs (e.g. culture, patient information security, patient information privacy, and patient information policies) that previous research studies suggest play a major role in implementing and adopting telemedicine.

2.1. Literature on Culture in Telemedicine

There are only a few research studies that consider culture as a construct in adopting telemedicine. We find the work of [1, 7] relevant when culture is considered as an antecedent for successful telemedicine adoption. A brief summary of these follows. Hu et al. (2000) suggest that telemedicine adoption involves both technological and managerial challenges [24]. The authors were able to demonstrate that the collective attitude of medical staff and perceived service risks were the most significant factors in telemedicine implementation.

Gagnon, Godin, and Gagne (2003) examined the linkage between Hofstede’s (2001) national cultural dimension of uncertainty avoidance and telemedicine implementation types [18, 23]. Based on their research in five countries, the authors suggest that national cultures with high uncertainty avoidance (e.g. France, Japan) favor a highly mechanistic implementation of telemedicine. On the other hand, cultures with low uncertainty avoidance (e.g., USA, UK) favor an organic organizational form of implementation of telemedicine adoption.

2.2. Literature on Information Security, Privacy, and Policies in Telemedicine

Threats related to information security are a major concern for many organizations since these risks may increase their liability and decrease their credibility [15]. The core difference between telemedicine and traditional healthcare is the use of the Internet, and therefore, online patient information security, privacy, and policies are of paramount concern. We discuss these issues in the following sections.

2.2.1. Literature on Patient Information Security in Telemedicine

Security objectives for communicating information over the Internet include mainly authentication, non-repudiation, and access control. Applying these procedures in telemedicine is not, however, as straightforward. Even though authentication and authorization procedures may keep patient information safe and secure, concurrently, they may impose boundaries on productivity and efficiency of healthcare professionals [32]. In this area, we find the models, procedures, and techniques provided by [32, 48] relevant and will be further addressed. Another model suggested by [32] revealed the relationship between clinical and administrative healthcare information systems adoption in an organization and technical information technology capabilities of the organization. The model includes factors related to market, policies, institutional, and technical capabilities. In general, the study showed that there should be more control regarding healthcare information security in hospitals. The results further indicated that size, IT infusion, and regulations impact healthcare information security.

Vaast (2007) performed a case study to understand how different members of different communities working in the same hospital understand healthcare information security [48]. Semi-structured interviews with 39 individuals employed in different healthcare occupations (physicians, registered nurses, medical residents, technicians, clerks, administrative associates, and IS professionals) were conducted. The results showed that, when related to patient information security, these communities do not have the same understanding of security.

2.2.2. Literature on Information Privacy in Telemedicine

Health care providers are increasingly using telemedicine for monitoring patients’ health [50]. Transferring personal health information between patients and provider, however, raises the issue of potential privacy violations of confidential patient information. The American Recovery and Reinvestment Act of 2009 imposed new privacy and security requirements on the old Health Insurance Portability and Accountability Act of 1996 (HIPAA) law. Healthcare information privacy, therefore,
A comprehensive and integrated model is needed to measure healthcare professionals' intention to adopt telemedicine. The model should integrate culture, patient information security, privacy, and policy toward successful implementation of telemedicine (see Figure 1). The proposed research model is grounded in Protection Motivation Theory (PMT), Rational Deterrence Theory (RDT), Hofstede’s Theory on Culture (TOC), and Moor’s Control Access Theory (CAT). Combining different theories, as done in this research study, is called theory integration. This integration is intended to fuse different theories, so that the integrated model provides more explanatory power than a model derived from a single theory [2]. In the next section, we briefly discuss PMT, RDT, TOC, and CAT, and illustrate why these theories are used in the present research and which constructs of these theories are utilized to create the proposed model.

PMT originated in health sciences and is aimed at motivating people to avoid unhealthy behavior through fear appeals [40]. PMT is divided into two parts: threat appraisal and coping appraisal. Threat appraisal evaluates how a person responds when he/she is faced with a threatening situation (e.g., a physician may be threatened by potential legal and financial ramifications, and decreased credibility if, upon adoption, security breaches take place in electronic patients records). Coping appraisal consists of two dimensions: self-efficacy and response efficacy. Self-efficacy refers to a person’s evaluation of his/her capability to deal with and avoid possible damage or loss that a threat may cause. Regarding telemedicine adoption, self-efficacy is the healthcare professional’s confidence in his/her ability to be able to use telemedicine. Response efficacy, on the other hand, suggests the effectiveness of a proposed action. Response efficacy, in the context of the present research, refers to a healthcare professional’s confidence about whether telemedicine security measures can prevent potential hackers from breaking into telemedicine databases and stealing patients’ health records. Based on PMT, we hypothesize that security measures such as confidentiality, authorization, authentication, and access control toward protecting electronic patient records will encourage healthcare professionals to adopt telemedicine.

Moor (1997), through his CAT, argued that a person has privacy in a situation concerning others if and only if in that situation the person is protected from intrusion, interference, and information access by others [35]. He further held that privacy right allows us to build close relationships with other individuals that could be difficult to build in public [35]. He described privacy as the core value of security and

2.3.3. Literature on Information Policies in Telemedicine. Regulations play a major role in decisions to implement distance healthcare. In the United States, HIPAA requires health care organizations to "maintain reasonable and appropriate, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information.". A number of research studies including a research paper by [31] have explored the impact of policies on telemedicine adoption.

Kiffe, Mbarika, and Tsuma (2008) empirically investigated the relationship between e-health policies and telemedicine capabilities [31]. Based on a Structural Equation Modeling (SEM) analysis on data collected from two hundred and twenty physicians and medical specialists, the authors found a strong relationship between security policies and telemedicine adoption. Conversely, the authors did not find a significant relationship between e-health policies and telemedicine adoption. In the next section, we discuss theoretical framework used in the present research.

3. Theoretical Framework

deserves serious consideration during any decision on adopting telemedicine. A number of researchers have addressed this issue in the past. Recent studies by [39, 53] are relevant to the present study and are addressed further.

Perera, Gihan, Holbrooka, Thaban, Fostera, and Willison (2011) empirically examine patients’ and physicians’ opinions about the privacy, benefits, and harms in using electronic health data for patient care and secondary purposes [39]. The results show that the majority of physicians and patients are not concerned about privacy loss and see more benefit in using electronic health records than paper based records. The study shows that privacy of electronic health records is not impacting the physicians’ decision to adopt this technology.

Zaidan and Zaidan (2011) conducted an empirical study on the impact of data privacy and confidentiality on telemedicine adoption [53]. Using survey research, the authors polled the participants asking them whether they “would mind if your health data is being available to others.” One hundred twenty eight out of 130 people who participated in the survey said they would mind. Based on these results, the authors recommend several items to protect patient privacy. Among them, they found designing and implementing secure algorithms using hybrid passwords with token or graphic passwords to be most useful.

2.3.3. Literature on Information Policies in Telemedicine. Regulations play a major role in decisions to implement distance healthcare. In the United States, HIPAA requires health care organizations to "maintain reasonable and appropriate, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information.". A number of research studies including a research paper by [31] have explored the impact of policies on telemedicine adoption.

Kiffe, Mbarika, and Tsuma (2008) empirically investigated the relationship between e-health policies and telemedicine capabilities [31]. Based on a Structural Equation Modeling (SEM) analysis on data collected from two hundred and twenty physicians and medical specialists, the authors found a strong relationship between security policies and telemedicine adoption. Conversely, the authors did not find a significant relationship between e-health policies and telemedicine adoption. In the next section, we discuss theoretical framework used in the present research.

3. Theoretical Framework

A comprehensive and integrated model is needed to measure healthcare professionals' intention to adopt telemedicine. The model should integrate culture, patient information security, privacy, and policy toward successful implementation of telemedicine (see Figure 1). The proposed research model is grounded in Protection Motivation Theory (PMT), Rational Deterrence Theory (RDT), Hofstede’s Theory on Culture (TOC), and Moor’s Control Access Theory (CAT). Combining different theories, as done in this research study, is called theory integration. This integration is intended to fuse different theories, so that the integrated model provides more explanatory power than a model derived from a single theory [2]. In the next section, we briefly discuss PMT, RDT, TOC, and CAT, and illustrate why these theories are used in the present research and which constructs of these theories are utilized to create the proposed model.

PMT originated in health sciences and is aimed at motivating people to avoid unhealthy behavior through fear appeals [40]. PMT is divided into two parts: threat appraisal and coping appraisal. Threat appraisal evaluates how a person responds when he/she is faced with a threatening situation (e.g., a physician may be threatened by potential legal and financial ramifications, and decreased credibility if, upon adoption, security breaches take place in electronic patients records). Coping appraisal consists of two dimensions: self-efficacy and response efficacy. Self-efficacy refers to a person’s evaluation of his/her capability to deal with and avoid possible damage or loss that a threat may cause. Regarding telemedicine adoption, self-efficacy is the healthcare professional’s confidence in his/her ability to be able to use telemedicine. Response efficacy, on the other hand, suggests the effectiveness of a proposed action. Response efficacy, in the context of the present research, refers to a healthcare professional’s confidence about whether telemedicine security measures can prevent potential hackers from breaking into telemedicine databases and stealing patients’ health records. Based on PMT, we hypothesize that security measures such as confidentiality, authorization, authentication, and access control toward protecting electronic patient records will encourage healthcare professionals to adopt telemedicine.

Moor (1997), through his CAT, argued that a person has privacy in a situation concerning others if and only if in that situation the person is protected from intrusion, interference, and information access by others [35]. He further held that privacy right allows us to build close relationships with other individuals that could be difficult to build in public [35]. He described privacy as the core value of security and
suggested that each individual needs it to survive. Based on CAT, we hypothesize that privacy and protection of patient records will motivate healthcare professionals toward telemedicine adoption. Furthermore, if patients feel comfortable about telemedicine being able to keep their health information private, they will feel comfortable about physicians adopting and using telemedicine.

RDT describes the behavior of an individual to control or prevent punishment or retribution. There are two groups of deterrence: general and specific. General deterrence focuses on policies. The person does not have to change his/her behavior, but will be punished in public if he/she violates such policies. Specific deterrence relies on the person making an effort to change his/her actions, if necessary, to avoid punishment. Beccaria (1963) believed that deterrent is beneficial considering certainty of sanction and severity of sanction [9]. According to this theory criminals would avoid unlawful behavior if the chance of getting penalized is high. We believe information privacy and security policies can have an impact on crime prevention if these policies are robust enough. Thus, these policies can prevent criminals from violating a patient’s privacy. Noncriminal, inadvertent and careless release of confidential records should also be reduced. Based on RDT, we hypothesize that adequate, organizational policies and procedures will deter hackers from violating a patient’s privacy and security which, in turn, will encourage healthcare professionals to adopt telemedicine.

Hofstede (2001) is very insightful when it comes to investigating the adoption of telemedicine [23]. He stated that organizational systems work best when their values and culture are consistent with the underlying values and culture of the society in which they are implemented [23]. He has identified four culture dimensions: Power Distance Index (PDI), Uncertainty Avoidance Index (UAI), Individualism Index (IDV), and Masculinity Index (MAS) [23]. PDI refers to what extent the equal distribution of power is accepted in a culture, while UAI represents the level of tolerance for uncertainty and ambiguity in the culture. IDV refers to the degree to which individual or collective relationships are reinforced in a culture, while MAS is the degree to which the traditional masculine values are reinforced in the culture. In the present research, our culture construct contains all four dimensions of Hofstede’s TOC [23]. In the next section, we put forward the research model and hypotheses.

4. Research Model and Hypotheses

Based on the previous discussion, we posit the following conceptual model (see Figure 1). The model offers an overview of the main constructs for telemedicine adoption. More specifically, our research model puts forth the impact of culture on telemedicine adoption. It also considers the impact of culture on patient information security, privacy, and policies. The model also examines the impact of patient information privacy, security, policy, and culture on the adoption of telemedicine.

Figure 1. Hypothesized model

4.1. Hypotheses

The following section describes the hypotheses used in the present research and provides the literature support for each hypothesis. Vroom and Solms (2004) reported that the human factor has an impact on maintaining information security [49]. According to the authors, organizational culture can help individuals become aware of security rules and policies and encourage the adoption of such policies [49]. Trimmer, Callucci, Wiggins and Woodhouse (2009) also investigated the impact of organizational culture on EMR acceptance in hospitals using a sample of physician residents [47]. The results of the study showed that organizational culture in hospitals has a positive and significant impact on strategic implementation of EMR.

Glaser (2009) examined the relationship between PDI, IDV, UAI, MAS and information security in different countries [19]. The author found that UAI influences information security. The impact is positive in some cultures and negative in others. We postulate, based on the aforementioned discussion, the following hypothesis:

H1: Culture, as defined by Hofstede, will directly influence patient information security needs for telemedicine adoption.
Ciganek and Francia (2009) found that countries with low UAI (e.g., Japan and Taiwan) are more likely to adopt and respond to policies and regulations to avoid uncertainty [16]. Solms and Solms (2004) believed that for a certain policy to work and to be effective, the rules have to be aligned to the culture of employees [43]. In view of the aforementioned discussion, we hypothesize:

H2: Culture, as defined by Hofstede, will directly influence patient information policy needed for telemedicine adoption.

The relationship between culture and privacy is somewhat mixed in the literature. Schmidt, Johnston, and Arnett (2008) found that there are important differences between countries with low UAI verses high UAI (e.g., USA vs. Taiwan) on their view of perceived computer privacy [41]. Ifinedo (2008), on the other hand, found no differences between an organization’s views on 13 key IT privacy and security issues in low and high UAI countries [25]. Consistent with the aforementioned discussions, we hypothesize:

H3: Culture, as defined by Hofstede, will directly influence patient information privacy needed for telemedicine adoption.

Harari, Norton, Lockwood, and Swift (2004) found that culture is a significant factor in the adoption and use of medical commerce [21]. They applied Hofstede’s culture dimensions to show why the adoption rate is lower in Hong Kong than in the UK. The study by [30] showed that in SSA countries, uncertainty avoidance (UA) has little influence on telemedicine adoption. This result contradicts the findings by [46] who demonstrated that cultures with high UA have more difficulty in adopting new technology. Bangert and Doktor (2003) also applied Hofstede’s culture dimensions to show that in a low uncertainty avoidance culture physicians were more formal and centralized (mechanistic organizational design) and needed to be more diverse and participatory (organic organizational design) for successful telemedicine adoption [6]. Nwabueze, Meso, Mbarika and Kifle (2009) also considered the effect of Hofstede’s dimensions on behavioral intention to use telemedicine in underserved countries [37]. The authors found that uncertainty avoidance has a powerful impact on prospective users' behavioral intention to use telemedicine but interestingly not on actual users. We postulate, based on the aforementioned discussion, the following hypothesis:

H4: Culture, as defined by Hofstede, will directly influence telemedicine adoption.

Jahangir and Begum (2008) investigated the impact of security on the adoption of electronic banking and found that security and privacy positively impact customers’ adoption of this technology [27]. Kifle et al. (2006), in an empirical study in SSA countries, showed that security policies have a significant and positive influence on telemedicine adoption [30]. In view of the aforementioned, we hypothesize:

H5: Information security will directly influence telemedicine adoption.

During the last five years, most national governments have developed information and communication technology (ICT) policies for healthcare, but the relationship between the existence of these policies and the adoption of telemedicine is not clear. In the United States, HIPAA in 1996 was the first national standard to protect a patient’s medical records [21]. Jennett, Scott, and Afleck (2004) emphasized the impact of policies on the adoption of electronic health records (EHR) [28]. They believe that one of the barriers to the adoption of EHR is the lack of agreement between political parties on how to spend the healthcare budget. In line with these research findings, we hypothesize:

H6: Patient information policies will directly influence telemedicine adoption.

Earp and Payton (2006) studied a group of healthcare professionals and found that these professionals are primarily concerned with errors in patient records in terms of improper access, unauthorized secondary use, and data collection errors [17]. Angst and Agarwal (2009) investigated the impact of privacy on the adoption of EHR [4]. The results of their study showed that patient privacy is the most important threat to the adoption of EHR. Terry and Francis (2007) also found the importance of privacy and confidentiality on HER’s usefulness in telemedicine adoption [45]. In connection with this, we hypothesize:

H7: Information privacy will directly influence telemedicine adoption.

In the healthcare arena, regulations play a major role in implementing patient information policies. In the United States, the HIPAA law of 1996 requires health care organizations to protect against potential privacy and security breaches of protected health information. In addition to HIPAA, the Health Power Act of 2001 allows states to upgrade their legal, technical, and public policy infrastructure to minimize the impacts of aforementioned breaches [8]. In view of this discussion, it is clear that patient information policy will dictate patient information privacy and security. We therefore hypothesize:

H8: Information policy will directly influence information security.

H9: Information policy will directly influence information privacy.

5. Methodology
Based on the existing research literature and Hofstede’s TOC, we designed an instrument to gather information on telemedicine adoption and culture. This instrument contains a total of the 49 questions. The first 24 questions were used to collect information on the security, privacy, policy, and telemedicine adoption constructs. The next 20 questions collectively measured the culture construct. These items were provided by Hofstede [23] as a part of his TOC. The respondents were asked to answer each question using a seven-point Likert-type scale with values ranging from 1 (strongly agree) to 7 (strongly disagree). The last five questions asked respondents to provide some demographic information. The instrument was hosted on Qualtrics and the respondents were asked to submit their answers anonymously using this web-based instrument.

5.1. Data Collection

The data used to test the hypothesized model were obtained by surveying about 300 physicians, physician’s assistants, nurse practitioners, medical students and residents, executives, and nursing professionals who also used telemedicine systems in the state in which data were collected. An electronic link to the instrument hosted on the Qualtrics was first sent to potential participants. They were asked to fill out the survey instrument. When a participant did not respond, an MD2 who is related to one of the authors took personal responsibility to deliver a hard copy of the questionnaire to the participant. He followed up with those who did not respond and asked them again to fill out the questionnaire. Nursing professors gave the questionnaire to nursing professionals who enrolled in their classes.

Taking into consideration the missing data and invalid responses, we had a total of 192 usable responses. Forty five percent of the respondents were males while 55% percent were females. Thirty four percent of the respondents were physicians, less than one percent were physician assistants, less than 1% nurse practitioners, 4% medical students, 3% percent medical residents, less than one percent executives, 1 percent information technology specialists, 43% percent nursing professionals and 11 percent others.

6. Fit and Model Reliability Statistics

Results on the model fitness, reliability, correlation matrix, and statistical significance of the hypotheses are presented in this section. We used AMOS-based Structural Equation Modeling (SEM) to analyze the hypothesized model because it offers numerous useful statistics [5].

6.1. Model Fit Statistics

There does not seem to be any agreement on a single measure of fit for the SEM analysis [34]. Thus, we present several measures including goodness-of-fit statistics which is a standard practice. The hypothesized model has a chi-square/df value of 2.75 with a p value less than 0.001 (see Table 1). This indicates a good fit of the model to the data collected for this research. Wheaton, Muthen, Alwin, and Summers (1977) suggested that a model has a good fit to the data if this value is less than 5.0 [51].

We next report the comparative fit index (CFI), as proposed by [10]. CFI is a non-centrality-based index which assumes that the possibility of a perfect fit between the model and the data is unlikely in the population because there is a possibility that some variables may have been inadvertently left out of the model [10]. CFI ranges in value from 0 to 1, with a value close to 0.90 serving as a limit for acceptable fit [20]. The proposed model, in the present research, has a CFI value of 0.72 which we believe falls within the acceptable range. The next index we report in this analysis is RMSEA. RMSEA considers the error approximation and addresses the question of how well the model fits the population covariance matrix, if it is available. The hypothesized model has an RMSEA of 0.10. Browne and Cudeck (1993) questioned the fit of models with an RMSEA less than 0.10 [12]. Overall, results related to the hypothesized model in Figure 1 suggest that it fits well to the data, with a $\chi^2/df = 2.75$, $p < .001$, CFI = .72 and RMSEA = .10.

Following a suggestion made by [33], we compared the present research model to an independence-model (null model) in which all variables are considered to be unrelated. Table 1 presents statistics for the two models, which shows that the hypothesized research model is superior to the independence model. In summary, indices and other statistics used in the present research suggest a good fit of the hypothesized model to the data.

<table>
<thead>
<tr>
<th>Table 1. Model fit statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
</tr>
<tr>
<td>Default model</td>
</tr>
<tr>
<td>Independence model</td>
</tr>
</tbody>
</table>

6.2. Reliability

---

2 We thank Babak Rajabi, MD for his help with collecting data.
We next determine the reliability of constructs used in the research instrument using Cronbach’s alpha. This is done to ascertain both stability and internal consistency of the instrument. Culture, information privacy, information security, information policy and adoption of telemedicine have reliability scores of 0.82, 0.87, 0.93, 0.81, and 0.86 respectively (please see Table 2). Nunally (1970) indicated that 0.70 is an acceptable level of reliability for a construct [36]. With the exception of culture, all other constructs meet the [36] benchmark. We intend to test the reliability of the instrument each time we administer it in a country.

6.3. Validity

We also validated the instrument to ensure that we measured what we intended to measure. We used convergent validity and discriminant validity to check the validity of the instrument.

6.3.1. Convergent Validity. In order to verify that all items loaded well in their assigned constructs, we used factor analysis with a reference norm of 0.40 as the ideal loading factor as suggested by [20]. Table 3 shows the results of this test. Thirteen of 20 items in the culture construct load well (≥ 0.40). All four items in the information privacy group load very well (≥ 0.68). All items in the information security group also load very well (≥ 0.72). All five items in the information policy group load very well (≥ 0.56). The average variance explained by each factor obtained from factor analysis communalities is 1.39, 0.24, 0.26, 0.28, and 0.25 for culture, privacy, security, policy, and adoption, respectively.

6.3.2. Discriminant Validity. Discriminant validity, according to [13], is the degree to which measures of different concepts are distinct. They suggest, in order to establish discriminant validity, correlations between items within constructs must be significantly greater (p < .05) than correlations among items between constructs (correlations among constructs are provided in Table 3). Correlations among items within the information security, privacy, policies, and telemedicine constructs were greater than .79, .53, .52, and .35, respectively (p<.05). Most of the correlations in culture construct were .20 or higher. All correlations among constructs are significantly correlated.

<table>
<thead>
<tr>
<th>Table 2. Scale development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Construct</td>
</tr>
<tr>
<td>Culture</td>
</tr>
<tr>
<td>Info. Privacy</td>
</tr>
<tr>
<td>Info. Security</td>
</tr>
<tr>
<td>Info. Policy</td>
</tr>
<tr>
<td>Adoption of Telemedicine</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3. Correlation analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Culture</td>
</tr>
<tr>
<td>Culture</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Privacy</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Adoption</td>
</tr>
</tbody>
</table>

* means significant at the .05 level, ** means significant at the .01 level, and *** means significant at the .001 level

7. Results

AMOS/SEM results showed coefficients for paths from culture to information security and telemedicine adoption are not significant. The paths from culture to information policy and privacy are significant at .01, .05 respectively. Similarly, the coefficients for the paths from information security and policy to telemedicine adoption were significant at the .10 and .01 levels, respectively. The path from information privacy to telemedicine adoption was not significant. The rest of the paths (e.g., information policy to information security and information policy to information privacy) were significant at the .10 and .01
levels respectively.

Figure 2. Results from the hypothesized model

* means significant at the .10 level, ** means significant at the .05 level *** means significant at the .01 level

8. Discussion and Recent Research

In order to generalize and effectively gauge telemedicine adoption success in a culture, one must identify a number of macro indicators and ascertain how they collectively affect this success. The AMOS-based SEM analysis of the present research, using data collected from the United States, indicates that the proposed model is able to partially explain telemedicine adoption success utilizing the constructs identified and grounded earlier using culture, information privacy, information policy, and information security literature and using the PMT, RDT, TOC, and CAT theories. More specifically, the present research empirically shows that telemedicine adoption is not directly and significantly affected by culture despite what we hypothesized (H4).

Several recent studies found a positive and significant relationship between culture and medical commerce adoption [22] in particular and new technology in general [46]; telemedicine adoption and information security [30]; electronic health records adoption and information policy [4], and electronic health records adoption and information privacy and confidentiality [45]. We were unable to validate the results of the aforementioned studies in the context of telemedicine adoption (see the results on H4).

We were, however, able to agree with [30] who stated that in SSA countries, UAI does not have much influence on telemedicine adoption since we were able to show that culture does not significantly affect telemedicine adoption.

The present research is unable to empirically validate the proposed impacts of culture on information security (H1), however, information policy (H2), and information privacy (H3) are impacted by culture.

According to [49], the organizational culture can help employees adopt security rules and policies. Glaser (2009) found that UAI influences information security [19]. Glaser (2009) also found this impact positive in some cultures and negative in others [19]. We were unable to validate, based on our results on H1, the findings of [19] and [49].

Ciganek and Francia (2009) believed that countries with low UAI are more likely to adopt and respond to policies and regulations [16]. Solms and Solms (2004) believed that for a certain policy to work and to be effective, the rules have to be aligned to the culture of employees [43]. We were able to agree in this regard, based on our findings on H2, with both the authors.

The relationship between culture and privacy, as stated earlier, is somewhat mixed in the literature. Schmidt, Johnston, Arnett, Chen, and Li (2008) found, when it comes to privacy, there are important differences between countries with low UAI versus high UAI [41]. Iffinedo (2008), on the other hand, found no differences between an individual’s views on perceived privacy in different cultures [25]. Our results confirm the results in [41].

The present research empirically shows that telemedicine adoption is also significantly affected by information security (H5), information policy (H6), but not information privacy (H7).

Kifle et al. (2006), in an empirical study in SSA countries, showed that security policies have a significant and positive influence on telemedicine adoption [30]. In view of our results on H5, we agree with these authors. Angst and Agarwal (2009) and Terry and Francis (2007) investigated the impact of patient information privacy and confidentiality on the adoption of EHR [4, 45]. The results showed that these issues play a very important role in EHR adoption. Our research, however, does not confirm, based on our empirical results on H7, that patient information privacy plays a significant role towards telemedicine adoption. Jennett, Scott, and Afleck (2004) asserted the importance of policies on the adoption of electronic health records (EHR) [28]. In view of our results on H6, we are able to empirically validate the assertion made by these authors.

Our results also support H8 and H9. This is consistent with the study of [11] methodology that allows patient information privacy and security requirements to be obtained from HIPAA.

9. Conclusions, Limitations, Implications and Future Research Directions
The literature suggests that culture plays an important role in telemedicine adoption. In order to address this important issue, the present research first posited a new theory-based comprehensive model to explain factors affecting telemedicine adoption. The model is derived by combining elements from PMT, RDT, TOC, and CAT. The model was then empirically validated using data collected from the United States. The results from the SEM-based data analysis show that culture does not play an important direct role in telemedicine adoption. Culture, however, indirectly influences telemedicine adoption through information privacy and information policy [30]. This leads to the conclusion that before telemedicine is brought in, it would be beneficial to consider the culture under which the telemedicine will function to make sure that there is a synergy between the two.

Our results also show that information security, privacy, and policy significantly impact telemedicine adoption. Information policy also positively and significantly impacts both information privacy and information security. These results are also supported by the literature.

This study presents three implications for practitioners: first, before bringing in telemedicine, authorities must consider the culture of the country and its policies under which the telemedicine will function to ensure that there is a synergy between the two. Second, before a telemedicine system is implemented, it is essential to have established security standards. Finally, information policies must be carefully looked at before a decision is made for telemedicine adoption.

The study is limited to culture and telemedicine as they exist in the United States. Other countries may have different results especially as influenced by their respective cultural norms. Future research can explore these relationships in other countries. By doing so, the implications for telemedicine adoption may be made available to practitioners and researchers in these other countries.

Finally, future research may compare the adoption of telemedicine and its relationship with cultural norms between various countries to gain a better insight into international differences.

10. References

References 48-53 are available from the second author on request.