Health Informatics Journal

Original Article

Health Informatics Journal
2020, Vol. 26(4) 2344–2361
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1460458220902957
journals.sagepub.com/home/jhi
SAGE

Telemedicine adoption issues in the United States and Brazil: Perception of healthcare professionals

Edimara Luciano
Pontifícia Universidade Católica do Rio Grande do Sul, Brazil

M Adam Mahmood
The University of Texas at El Paso, USA

Parand Mansouri Rad
California State University, USA

Abstract

Telemedicine has recently garnered more attention from healthcare professionals because it provides access to health services to patients in rural areas while making patient healthcare information more vulnerable to security breaches. The objective of this research is to identify factors that play a critical role in possible adoption of telemedicine in the United States and Brazil. A model with eight hypotheses was used to establish a research framework. A survey was conducted involving healthcare professionals in the aforementioned countries. The results show that telemedicine adoption is influenced by policies and culture in both countries and influenced by security and privacy in the United States. It can be inferred from the research that perceptions of the American and Brazilian healthcare professionals are similar in telemedicine issues covered in this research. These healthcare professionals, however, disagree on how patients' privacy should be preserved in the two countries.

Keywords

adoption, barriers, ehealth, electronic health records, telehealth, telemedicine

Corresponding author:
Parand Mansouri Rad, California State University, Chico, Chico, CA 95929-0001, USA.
Email: pmansouri-rad@csuchico.edu

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

Introduction

The healthcare sector has been experiencing major challenges around the world, such as rising costs, increasing demands of patients, and universal access.[1] Telemedicine can be an alternative to deal with these challenges since it provides a solution to the problems of accessing healthcare, especially in developing countries where healthcare professionals are not as readily available.[2] Telemedicine is defined by the American Telemedicine Association[3] as the remote delivery of healthcare services and clinical information using telecommunications technology, such as the Internet, wireless networks, intranets, and extranets. Telemedicine has been used in the healthcare business since the early 1960s[4] and underwent several cycles of increasing and decreasing interests. Telemedicine has recently gained more attention because it provides more access to health services but, at the same time, it makes patient health information vulnerable to security and privacy breaches. In addition to security and privacy issues, state licensing policies can create a challenge for healthcare professionals who practice telemedicine, since they are not allowed to treat patients in states other than where they are licensed. Each healthcare professional should follow laws and requirements in the state where the patient is receiving health services. As a result, states laws and regulations pose a major barrier in adoption of telemedicine in regions who need it the most.

Health services are very specialized, normally expensive, and frequently concentrated in some areas in a country or perhaps in a part of the world. Because of this, it is difficult and costly to provide high-quality, face-to-face health services.[5] This provides an opportunity for the adoption of telemedicine, which requires the use of high-level information technology (IT). The adoption of an IT-based solution brings consequences (expected and unexpected), to the users,[6] and with telemedicine users, it is no different. According to the authors, these consequences are interpreted and understood in various ways by users, triggering reactions from them. This study focuses on the issues involved in putting telemedicine into practice.

Dünnebeil et al.[7] suggest that the main reasons for opposition to the adoption of distance healthcare (DHC) are privacy concerns, the extensive efforts required to implement the project, and dissatisfaction with the performance of the technology. Chang et al.[8] describe problems with poor security, confidentiality, and reliability. Ekeland et al.[9] call attention to the importance of policies as a way to define how telemedicine can be used. Barlow et al.[10] and Saliba et al.[11] suggest the culture as a barrier for telemedicine diffusion, creating mistrust and resistance by means of incompatibilities with values and cultural norms of a society. Based on this, the adoption issues examined in this study are information security, privacy, policy, and national culture.

The objective of this research is to identify factors that play a critical role in the possible adoption of telemedicine. More specifically, this research will focus on the perception of healthcare professionals on the influence of issues such as security, privacy, policies, and culture on telemedicine adoption. This research is based on a survey involving physicians, nurses, medical students, medical residents, and IT professionals from the United States and Brazil. A two-country study was used as a way to contribute to the understanding of why telemedicine is more accepted in some societies over others. Most telemedicine research studies have focused on the technology and clinical issues; consequently, there has been limited discussion of managerial issues. Similarly, most research studies considered the patients' point of view. This research will consider the healthcare professional's perspective. Telemedicine adoption must consider the managerial viewpoint because of the high amount of investments and significant changes in the routine of healthcare professionals.

The rest of the article is structured in the following manner: the next section details the theoretical background of telemedicine. This is followed by a description of the research methodology and the results. The article closes by providing conclusions and implications drawn by this research.

Background

This section provides the literature background upon which this research is established. More specifically, it covers telemedicine issues.

Telemedicine adoption

In order to achieve a successful DHC adoption, it is mandatory to consider that there are different people or groups of people involved. They may have different perceptions and sometimes even divergent opinions on what factors are critical in DHC adoption. This can become more complicated due to the interactions necessary between multiple factors[12] with different concerns about cost-effectiveness, quality of care, privacy, and preference for regular care instead of DHC.[8]

Dünnebeil et al.[7] conducted research in Germany and concluded that the perceived importance of standardization and the perceived importance of the current IT utilization were the most significant drivers for accepting DHC. Perceived importance of information security and process orientation was also viewed as important.

Chau and Hu[13] perceived some differences between DHC adoption by healthcare professionals and researchers. The authors argued that healthcare professionals are more pragmatic during the decision-making process to adopt DHC. They tended to focus on the technology's usefulness more than on its ease of use. These professionals seemed to be relatively independent in making technology acceptance decisions while considering suggestions from others.

Tarakci et al.[14] further noted that there were no frameworks that could aid in defining the appropriate approach, scope, and application of telemedicine adoption in different contexts. They also stated that an "important question as to 'how should we do this?' was still unanswered." This creates a limitation because the adoption of telemedicine involves making decisions on complicated matters. Hendy and Barlow[15] observed different levels of effectiveness for different phases of adoption. Their study showed that key aspects of organizational changes were highly effective in the first phase of adoption. This effectiveness worsened as the project reached the final phase.

Infrastructure

Today, telemedicine can be brought to any room with robots and monitors. Studies by Adelakun[16] and Kifle et al.[17] reveal that quality and availability of information and communication technologies (ICT) infrastructure is essential in adopting telemedicine. The authors argue that poor health infrastructure has negative impact on telemedicine adoption.

Moreover, in the survey published by World Health Organization,[18] 50 percent of the responding nations believe that lack of basic infrastructure such as power and water supplies is a barrier to telemedicine adoption.

Technology

Channels that are available for the exchange and transmission of health information are the essential part of telemedicine. Dinesen et al.[19] provide an international overview of telemedicine adoption and emphasize that technology plays an important role to achieve telemedicine adoption goals (improvement of quality of care and outcome and reducing the cost of care).[20]

Today, revolution of smart phones, self-tracking technologies, and increased access to wireless data make adoption of telemedicine more accessible. In terms of the number of Internet users, both the United States and Brazil are on the top five Internet market in the world.[21] Moreover, in both countries, more than 90 percent of the population use smartphones.

Economy

In developing countries such as Brazil,[22] telemedicine applications are more demanding and in some cases considered as an alternative or sometimes the only option. In developed countries like the United States, telemedicine is usually used as an addition to the traditional healthcare.[23] In both developed and developing countries, telemedicine is used when specialized physicians are not available in rural areas.

The study by Ranganathan and Balaji[24] examined the key predictors of telemedicine adoption and found that the chance of telemedicine adoption is lower when expensive equipment is needed for the healthcare organization and their demand is low. On the other hand, there is higher rate of adoption when clinics need remote medical monitoring rather than costly devices. The adoption rate is also higher when there is acceptable coverage or reimbursement.

Adler-Milstein et al.[25] examined the data gathered from Information Technology Supplement to the American Hospital Association's 2012 and found that rates of telemedicine adoption vary in each state. According to the authors, states that their policies encourage reimbursement for telemedicine practices have higher rate of adoption. On the other hand, requiring special license for out-of-state providers limits telemedicine adoption.

Organization

The assessment by Adler-Milstein et al.[25] reveals that chance of adoption of telemedicine is higher in clinics that are part of larger organizations, since they can profit from servicing various patients, needs, and locations. In addition, the authors demonstrate that teaching hospitals and more technology advanced organizations show more interest in adopting telemedicine.

Security issues

Baltzan[26] defines information security as "the protection of information from accidental or intentional misuse by persons inside or outside an organization" (p. 155). Potential threats to information security are hackers and viruses. Security in healthcare is still a big concern in the adoption of telemedicine.[27] Telemedicine information travels over the Internet, thus security is a big concern. With the recent expansion in ICT, telemedicine has been implemented in numerous areas in the medical field[28] resulting in concerns about the security of this information. Because of this, the adoption and use of IT in healthcare should be carefully tracked to ensure that confidentiality, access control, authentication, and authorization procedures are followed properly.[29]

The research of Chang et al.[8] describes the problem with poor security, confidentiality, and reliability provided by caregivers. The absence of adequate procedures to control access to, and use of, patient records can compromise the adoption of telemedicine. The use of different types of technology to access patient records is another challenge. Records accessed by mobile devices, for example, are subject to possible theft, unauthorized access, or even malicious attacks.[30]

Privacy issues

Privacy is

> the right to be left alone when you want to be, to have control over your own personal possessions, and not to be observed without your consent. Privacy is related to confidentiality, which is the assurance that messages and information remain available only to those authorized to view them.[26] (p. 143)

In use of telemedicine, the possible threat is the exposure of patients' information and unauthorized access to their medical records.[31] Dünnebeil et al.[7] stated that the main reasons given for opposition to the use of DHC are privacy concerns. Privacy concerns can also turn into ethical problems.[8] Moreover, Ali et al.[31] believed that when appropriate security measures are not met, the privacy of patients' medical records can be at risk and proposed a new algorithm for protecting electronic medical records (EMRs).

Another concern about privacy is disagreement on what information should be kept private. Different countries and societies have different thresholds.[32]

In order to guarantee that privacy is maintained in the United States, companies are required, for example, to comply with privacy and security laws as dictated by the Health Insurance Portability and Accountability Act (HIPAA).[33] HIPAA[33] specifies the type of healthcare information that should be kept private and to whom that information can be disclosed. This act also specifies administrative, physical, and technical safeguards required to protect healthcare information.

Policy issues

Policies ensure that telemedicine success results in fewer risks for the stakeholders and shareholders. Policies can be established by the government, associations, or companies. The policies dictate standards of operations, roles, and responsibilities the telemedicine services must operate under. Policies can determine how telemedicine can be used to reduce healthcare costs,[9] establish reimbursement guidelines, and detail how IT can be used to support telemedicine services. It is also important that, in order to comply with healthcare policies, a telemedicine coordinator with managerial skills is appointed.[34] This coordinator can work as a catalyst and is primarily responsible for the policies implementation and pursuance. Ekeland et al.[9] state that, despite a large number of research studies on telemedicine, evidence to support policy decisions is still lacking. This field, therefore, presents new opportunities for studies that involve guidelines for telemedicine adoption.[14]

Cultural issues

Culture can affect the adoption of an IT solution.[35] Barlow et al.[10] identified culture as a barrier to telemedicine diffusion. The authors also mentioned that cultural resistance has resulted from incompatibilities between the new IT regarding the values and cultural norms of an organization and the degree to which its results are visible to the potential adopter. Saliba et al.[11] explained that the language differences between the patients and healthcare professionals could generate mistrust resulting in resistance. Saliba et al.[11] also mentioned that in some cultures it could be considered as a failure on the part of doctors to ask for assistance or second opinions, especially if it involves a cross-border telemedicine service.

Hofstede[36] conducted a large study about national culture, aiming to identify value dimensions across cultures. He also developed work-goals brought up by questions with the format "How important is it to you?" This part of the questionnaire involves eight questions about the importance of some aspects of professional life (time for family, good physical working conditions, stability, etc.), six about the importance of some aspects of private life, and six more general questions about trust, society values, and rules.

As stated earlier, culture has an impact in telemedicine adoption and use, and this impact can act in different ways in the two countries selected for this research.

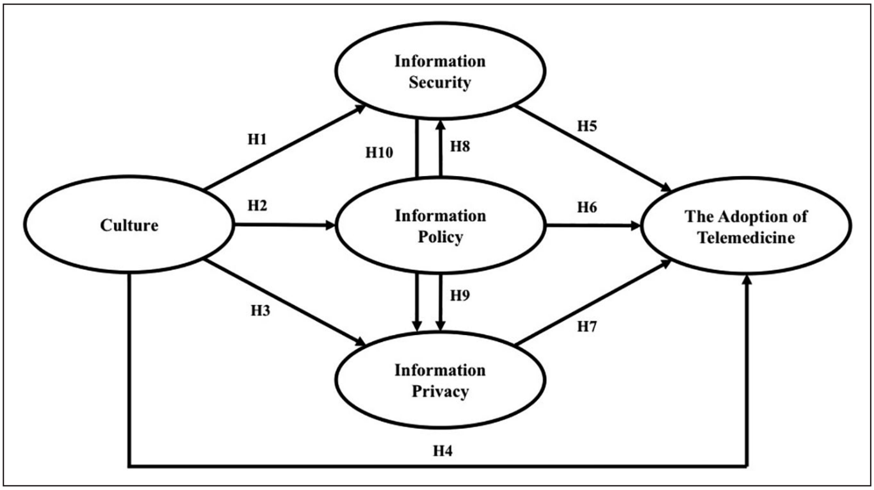

Figure 1. Issues in telemedicine adoption model.

Theoretical framework

Most of the studies on telemedicine adoption use either the Theory of Planned Behavior (TPB) or the Technology Acceptance Model (TAM). Therefore, a comprehensive and integrated model is needed to measure healthcare professionals' intention to adopt telemedicine. This model should integrate culture, patient information security, privacy, and policy toward successful implementation of telemedicine (see Figure 1). The proposed research model is grounded using the 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 study, is called theory integration.

The PMT, which originated in health sciences, aims at motivating people to avoid unhealthy behavior through fear appeals.[37] Threat appraisal evaluates how a person responds when he or she is faced with a threatening situation (e.g. a physician may be threatened by potential legal and financial ramifications and a decrease in credibility if, upon adoption security breaches take place in electronic patients' records). Based on PMT, current research hypothesizes that security measures, such as confidentiality, authorization, authentication, and access control toward protecting electronic patient records will encourage healthcare professionals to adopt telemedicine.

Through his CAT, Moor[38] argues that if a person is protected from interference, intrusion, and information access by other people, a person is said to have privacy. Moor[38] further discusses that this right allows us to build relationships with individuals that are hard to build in public. Based on CAT, current research hypothesizes that privacy and protection of patient records will facilitate 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.

RRDT describes the behavior of an individual to control or prevent punishment or retribution. RDT emphasizes the person making an effort to change his or her actions, if necessary, to avoid punishment. According to this theory, criminals would avoid unlawful behavior if the chance of getting penalized were high. Based on RDT, current research hypothesizes 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's TOC (2001) is very insightful when it comes to investigating the adoption of telemedicine. Hofstede[36] states clearly and emphatically 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. Hofstede identifies four culture dimensions as previously discussed.

Research model and hypotheses

Based on the previous discussion, the authors present the following conceptual model (see Figure 1). The model offers an overview of the main constructs, including the hypotheses, described below.

Alfawaz et al.[39] show that national culture traits (e.g. Hofstede's power distance dimension) have an influence on individuals' information security-related behavior in a case study in Saudi Arabia. Ifinedo,[40] however, found no significant differences between a national culture and individuals' perception of IT security in global financial services institutes. This research postulates, based on the aforementioned discussion, the following hypotheses:

H_1. Healthcare professionals' national culture influences information security.

Ifinedo[41] considered the impact of TPB on information system's security policy compliance. This study showed that subjective norms and the individual's attitude toward information security policies significantly influenced the intention to follow the privacy policies. Höne and Eloff[42] discuss that information security policies will have to match with the culture of the organization, and these policies should be flexible enough to be changed as the culture changes. In view of the aforementioned discussion, this research hypothesizes:

H_2. Healthcare professionals' national culture influences information policy.

Krasnova and Veltri[43] examined the influence of culture on privacy concerns in social network websites. Their study showed that countries with higher uncertainty avoidance, such as Germany, are less likely to adopt new technology. Bansal et al.[44] examined Hofstede's dimension and individualism, and found no impact of this dimension on health information privacy. However, they found a strong relationship between feminism and privacy of healthcare information. This research hypothesizes, based on the aforementioned discussion, the following hypotheses:

H_3. Healthcare professionals' national culture influences information privacy.

Culture can act as a barrier to telemedicine diffusion.[10] The cultural influence when adopting an IT solution is well known, since telemedicine involves a high level of IT according to Kappos and Rivard.[35] Furthermore, the most important issue is what is perceived as important, correct, and valuable for people influenced by the values, behaviors, and standards of their culture,[36] especially considering that different countries and societies have different thresholds.[32] For example, Saliba et al.[11] mentioned that in some cultures it could be considered a failure to ask for assistance or a second opinion, especially if it involved a cross-border telemedicine service. According to Barlow et al.,[10] this situation can occur because of the incompatibilities between the means used and the values and cultural norms. Jayasnighe et al.[45] also noted a relationship between culture and telemedicine adoption. Based on above studies, this research hypothesizes:

H_4. Healthcare professionals' national culture influences telemedicine adoption.

Since healthcare organizations have increased the use of IT in general, and telemedicine in particular, keeping patients' medical records secure has been a concern.[31] Therefore, the adoption and use of IT must be carefully followed to ensure that patient information security is preserved.[29] This is especially important because patient records are accessed from different types of dispositive.[30] The concern about patient information security can hinder the adoption of telemedicine. In view of the aforementioned discussion, this article hypothesizes the following:

> *H_5*. Healthcare professionals' security perception influences telemedicine adoption.

Healthcare policy will establish some standards of operations, roles, and responsibilities that are fundamental to telemedicine adoption, to the same extent that it reduces the perceived risk by stakeholders. Policies will dictate patient information privacy and security[14] and can establish the operation model, specifying standards about healthcare costs,[9] reimbursement guidelines,[46] and the role of IT.[47] Policies may also be influenced by cultural issues. Based on this, this research article puts forth the following hypothesis:

> *H_6*. Healthcare professionals' policies perception influences telemedicine adoption.

Privacy is one of the primary reasons given by healthcare professionals for opposing the use and adoption of DHC.[7] Healthcare professionals might think that the adequate procedures for ensuring data privacy, confidentiality, and reliability do not exist in telemedicine.[48] The protection of privacy and confidentiality is therefore a critical issue while adopting telemedicine,[30] especially about unauthorized access.[31] Based on this, this article hypothesizes:

> *H_7*. Healthcare professionals' privacy perception influences telemedicine adoption.

In the healthcare arena, regulations play a major role in implementing patient information policies. In the United States, the HIPPA law of 1996 requires the healthcare organizations to protect against potential privacy and security breaches into protected health information. In addition to HIPPA, the Health Power Act of 2001 allows states to upgrade their legal, technical, and public policy infrastructure to minimize the impacts of aforementioned breaches.[49] In view of this discussion, it is clear that patient information policy will dictate patient information privacy and security. Fernando and Dawson[50] believed that confusing and contradictory privacy and security laws impact the patients' health information security. Consistent with the aforementioned discussion, this research hypothesizes:

> *H_8*. Healthcare professionals' policy perception influences information security.
>
> *H_9*. Healthcare professionals' policy perception influences information privacy.

According to Kruse et al.[51] health records could be protected from unauthorized users when there are security measures such as physical safeguards (locks on laptops or room) and technical safeguard (encryption, firewalls). These security measures are essential to protect the patients' information privacy.[51] Damschroder et al.[52] argue that data security is an essential element of full privacy measures. Based on the above discussion, this article hypothesizes:

> *H_{10}*. Healthcare professionals' security perception influences information privacy.

Methodological procedures

Based on the model provided in Figure 1, a literature review of DHC, and Hofstede's theory on national culture, an instrument was designed to gather information on telemedicine adoption in the United States and Brazil (see Supplemental Appendix 1). This instrument contains a total of 44 questions. The first 19 questions were used to collect respondents' perceptions on security, privacy, policy, and adoption constructs and were based on the following research papers: D'Arcy et al.,[29] Ali et al.,[31] Ekeland et al.,[9] and Chang et al.[8]

The appropriation of the questions from the cited research papers and the fit for this research were discussed with a group of American health professionals who use telemedicine. Therefore, these professionals worked as experts, helping the researchers in preparing the questionnaire. The next 20 questions collectively measured the culture construct. These items were provided by Hofstede[36] as a part of his theory to identify international differences in work-related values. The respondents were anonymously asked to answer each question using a 7-point Likert-type scale with values ranging from 1 (strongly disagree) to 7 (strongly agree). The last five questions asked the respondents to provide some demographic information.

These two countries were chosen for convenience and also because each country is at a different stage in telemedicine adoption. The United States is an example of a typically developed country, whereas Brazil is still a developing country.

The instrument for collecting data was hosted on Qualtrics, and respondents filled out the survey using a link to the survey and submitted their answers online. An electronic link to the instrument hosted on the Qualtrics was first sent to potential participants. The participants were asked to fill out the survey instrument. Respondent's anonymity was maintained throughout the data collection process.

In the United States, the data were obtained by surveying approximately 300 physicians, physician's assistants, nurse practitioners, medical students, medical residents, healthcare executives, nursing professionals, and IT specialists who also used telemedicine systems in the state in which data were collected. Taking into consideration the missing data and invalid responses, there were a total of 192 usable US responses. In Brazil, the instrument was distributed to 148 physicians, physician's assistants, nurse practitioners, medical students, medical residents, nursing professionals, and IT specialists. After disregarding the questionnaires with missing responses, there were a total of 115 fully completed questionnaires.

The data from the United States showed that 86 percent of the respondents were males while 14 percent were females. However, in Brazil 45 percent of the respondents were males while 55 percent were females. About 60 percent of the Brazilian respondents had work experience between 1 and 5 years, 5 percent had between 6 and 10 years, 18 percent had between 11 and 15 years, 10 percent had between 16 and 20 years, and 7 percent had over 20 years. In the Brazilian sample, 47 percent of the respondents were medical students and the rest were IT specialists. In the data from the United States, 34 percent of the respondents were physicians, 1 percent were physician assistants, 1 percent were nurse practitioners, 43 percent were nursing professionals, 4 percent were medical students, 3 percent were medical residents, 1 percent were healthcare executives, 1 percent were IT specialists, and 12 percent were others.

Results

Reliability and validity

Cronbach's alpha was first utilized to determine the reliability of the constructs used in this research (see Table 1). The reliability ascertains both stability and internal consistency of the instrument.

Table 1. Scale development.

Construct (number of items)	Country	Mean, standard deviation, Cronbach's alpha	Factor loadings	Variance extracted
Adoption (5)	United States	30.05, 4.96, 0.859	0.91, 0.92, 0.56, 0.59, 0.59	0.25
	Brazil	26.62, 4.017, 0.525	1, 1.31, 0.40, 0.60, –0.008	0.16
Privacy (4)	United States	24.54, 4.87, 0.870	0.70, 0.91, 0.82, 0.68	0.24
	Brazil	21.82, 5.32, 0.814	0.83, 0.79, 0.64, 1	0.28
Information security (5)	United States	31.60, 5.1, 0.930	0.72, 0.86, 0.96, 0.95, 0.79	0.26
	Brazil	29.97, 5.06, 0.867	1, 1, 1.07, 1.13, 1.02	0.26
Policy (5)	United States	27.66, 5.26, 0.808	0.58, 0.82, 0.95, 0.67, 0.51	0.28
	Brazil	27.37, 4.498, 0.737	0.1, 1.50, 1.07, 2.25, 2.47	0.20
Culture (20)	United States	92.58, 11.8, 0.823	0.90, 0.74, 0.78, 0.90, 0.74, 0.84, 0.87, 0.85, 0.78, 0.82, 0.75, 0.71, 0.30, 0.40, 0.15, 0.19, 0.14, 0.24, 0.15, 0.15	1.39
	Brazil	104.83, 9.017, 0.668	0.79, 0.78, 0.59, 0.48, 0.69, 0.41, 0.74, 0.28, 0.69, 0.57, 0.72, 0.40, 0.003, 0.06, –0.13, –0.08, –0.01, 0.13, 0.12, –0.17	0.81

The values presented in Cronbach's alpha analysis are considered high, indicating a reliable questionnaire.

For the United States, the adoption, culture, information privacy, information security, and information policy have reliability scores of 0.82, 0.87, 0.93, 0.81, and 0.86, respectively. For Brazil, the culture, information privacy, information security, information policy, and adoption have reliability scores of 0.67, 0.81, 0.87, 0.74, and 0.52, respectively. Nunnally[53] indicates that 0.70 is an acceptable level of reliability for a construct. The US constructs meet Nunnally's benchmark. Brazilian constructs, with the exception of one construct, also meet Nunnally's benchmark.

The instrument was also validated to ensure that the study appropriately measured its intended objects. Convergent validity and discriminant validity were used to check the validity of the instrument. In order to verify that all items loaded well in their assigned constructs, factor analysis was used with a reference norm of 0.40 as the ideal loading factor, as suggested by Hais et al.[54] Eleven of 20 items for Brazil and 13 for the United States in the culture construct loaded well (⩾0.40). All five items in the information security group loaded very well for the countries (⩾0.72). Moreover, items in the information privacy group loaded very well for the two countries (>0.64). All five items in the information policy group loaded well for the United States (>0.51). Finally, all five items in the adoption construct loaded very well for both countries (⩾0.40). The average variance explained by each factor obtained from factor analysis communalities for the United States is 1.39, 0.24, 0.26, 0.28, and 0.25, and for Brazil, it is 0.81, 0.28, 0.26, 0.20, and 0.16, for culture, privacy, security, policy, and adoption, respectively.

Correlation analysis

A correlation test was used to understand the influence among adoption and the dependent variables. Table 2 provides the results.

According to Campbell and Fiske,[55] discriminant validity is the degree to which measures of different concepts are distinct. The authors suggest, in order to establish discriminant validity,

Table 2. Correlation analysis.

Construct/country		Culture	Policy	Privacy	Security	Adoption
Culture	United States	1.00				
	Brazil	1.00				
Policy	United States	0.52***	1.00			
	Brazil	0.48***	1.00			
Privacy	United States	0.44***	0.48***	1.00		
	Brazil	0.01	0.33***	1.00		
Security	United States	0.25***	0.025***	0.36**	1.00	
	Brazil	0.31***	0.48***	0.31**	1.00	
Adoption	United States	0.28***	0.60***	0.38***	0.28**	1.00
	Brazil	0.23***	0.36***	0.11	0.14	1.00

**Significant at the 0.05 level.
***Significant at the 0.01 level.

correlations between items within constructs must be significantly greater ($p < 0.05$) than correlations among items between constructs (correlations among constructs are provided in Table 2). For the United States, correlations among items within the information security, privacy, policies, and telemedicine constructs were greater than 0.79, 0.53, 0.52, and 0.35, respectively ($p < 0.05$). For Brazil, most of the correlations among items within the information security, privacy, policies, and telemedicine constructs were greater than 0.45, 0.39, 0.22, and 0.02, respectively ($p < 0.05$). Most of the correlations in culture construct were 0.20 or higher in the two countries. Correlations among constructs for both countries are shown in Table 2. All correlations among constructs are significant in the United States; however, for Brazil, correlations between culture and privacy, privacy and adoption, and security and adoption were not significant.

Structural equation modeling

Figure 2 shows the result for the hypothesized model for the United States and Brazil. Analysis of moment structures (AMOS)/structural equation modeling (SEM) results reveal that the path coefficient from culture to information security (H_1) is significant at the 0.05 level for the United States but not for Brazil. The path coefficient from culture to information policy (H_2) is significant for both countries at the 0.01 level. The results also indicate that the path coefficient from culture to information privacy (H_3) is not significant for the United States or Brazil. The results further reveal that there is not a significant path coefficient from culture to telemedicine adoption (H_4) for the United States or Brazil. The path coefficient from information security to telemedicine adoption (H_5) is significant for the United States only at the 0.10 level. Both countries have significant path coefficients from information policy to telemedicine adoption (H_6) at the 0.10 level for Brazil and 0.01 for the United States. It is interesting to note that none of the countries have a significant path coefficient from information privacy to telemedicine adoption (H_7). All the path coefficients from information policy to information security (H_8) and information privacy (H_9) are significant for both countries at less than the 0.10 level or lower. Finally, the path coefficients from information security to information privacy (H_{10}) are significant at less than 0.10 level for both countries.

Differences between countries using T-test

The T-test was also used to verify differences between the United States and Brazil in terms of the constructs used in this research (see Table 3).

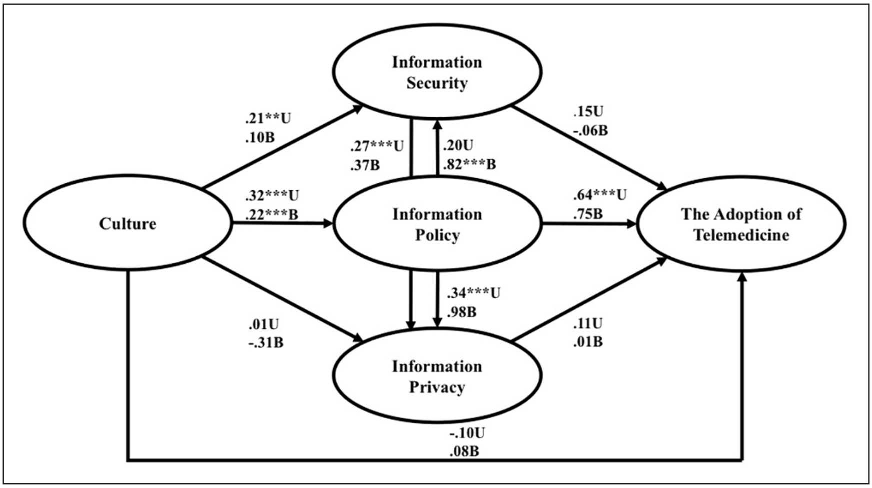

Figure 2. Results from the hypothesized model.
**Significant at the 0.05 level.
***Significant at the 0.01 level.

Table 3. T-test.

Construct/country		Paired samples				
		Statistics	Correlations	Test		
		Mean Standard deviation	Correlation Significance	Mean Standard deviation	T	Sig. (2-tailed)
Culture	United States	90.48 13.47	0.028 0.771	13.94 16.04	−8.990	0.000
	BR	104.8 9.10				
Privacy	United States	23.89 5.42	−0.051 0.592	2.17 7.79	2.934	0.004
	BR	21.72 5.32				
Security	United States	31.43 5.25	0.53 0.579	1.54 7.14	2.285	0.24
	BR	29.88 5.11				
Policy	United States	27.49 5.49	−0.37 0.706	0.137 7.25	0.198	0.000
	BR	27.35 4.53				
Adoption	United States	29.54 5.14	−0.13 0.894	2.96 6.59	0.198	0.000
	BR	26.57 4.06				

BR: Brazil.

Table 4. Multivariate tests.

Effect	Value	F	Error df	Sig.	Partial eta-squared
Country Pillai's trace	0.358	31.654	1452.000	0.000	0.179
Wilks' lambda	0.656	33.981	1450.000	0.000	0.190

T-test results present that policy, adoption, and culture have high statistical significance, and privacy was also significant. Security was not statistically significant between the United States and the Brazil sample, which indicates no difference between the groups. Based on this, it can be concluded that there are significant differences between the two countries in terms of perceptions on adoption, culture, policies, and privacy, but not on security.

Manova result

According to Swanson and Holton,[56] a Manova test is done to create a linear combination of dependent variables to maximize group differences. A test is performed to examine whether those differences are significant. The objective here is to examine whether there are significant mean differences between information security, information privacy, information policy, and telemedicine adoption among both countries. The multivariate analysis shows that overall there are significant differences among the countries in terms of privacy and policy (see Table 4).

A multiple comparison test was also performed and the results show that mean scores for security were statistically significantly different between the United States and Brazil ($p < 0.01$). Mean scores in privacy were statistically different between the United States and Brazil ($p < 0.0005$). Mean scores in policy were not statistically different between the United States and Brazil ($p = 0.828$). Mean scores for telemedicine adoption were statistically different between the United States and Brazil ($p < 0.0005$). Mean scores for culture were statistically significantly different between the United States and Brazil ($p < 0.0005$).

Discussion

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 this research, using data collected from the United States and Brazil, indicates that the proposed model is able to explain telemedicine adoption success. The proposed model utilizes 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.

This research demonstrates the proposed impacts of culture on information security in the United States but not in Brazil (H_1). The result from the United States is aligned with the study by Alfawaz et al.[39] who show that national culture traits (e.g. Hofstede's power distance dimension) have an influence on individuals' information security-related behavior.

The result of this research indicates that culture has a positive and significant impact on information policy in both countries, supporting H_2. This means the findings are in line with Jayasnighe et al.[45] who believe that culture impacts how privacy policies are perceived.

The results of this research suggest that information privacy is not affected by culture in the United States or Brazil (H_3). The result is aligned with the research by Ifinedo,[40] who believes that there are no differences between an individual's views on perceived privacy in different cultures.

This research empirically demonstrates that telemedicine adoption in the United States and Brazil is not directly and significantly affected by culture, despite what is hypothesized (H_4). Jayasnighe et al.[45], however, noted a significant relationship between culture and telemedicine adoption in Sri Lanka.

This research empirically shows that the impact of information security on telemedicine adoption is near significant (significant at the 0.10 level) in the United States but not in Brazil (H_5). However, Kruse et al.[57] considered security as a barrier to telemedicine adoption in some countries.

The results of this research show that the information policies in both countries significantly and positively impact telemedicine adoption, supporting H_6. The multiple comparisons test results indicate that there is a significant difference in adoption of telemedicine in Brazil and the United States. Research by LeRouge and Garfield[12] showed that having privacy regulations for patients' information lowers adoption of EMRs. The results from both countries empirically validate the assertion made by LeRouge and Garfield.[12]

The results of this research demonstrate that information privacy does not significantly impact adoption of telemedicine in both countries (not supporting H_7). This is an interesting finding because privacy of patient records should be of paramount concern to all involved in telemedicine adoption. Kruse et al.[57] also believed that privacy of patients in electronic health records impacts the decision to adopt telemedicine in the United States and the United Kingdom.

This research results reveal that the impact of information policy on information security is significant in Brazil and near significant in the United States. Furthermore, the impact of information policy on information privacy is significant in the United States and near significant in Brazil. The result partially supports H_8 and H_9. The multiple comparisons test results show that there is a significant difference in policy between Brazil and the United States. The result is partially in line with a study by Nikkhah and Sabherwal,[58] which showed a relationship between information security and policy.

Finally, the results of this research demonstrate that the impact of information security on information privacy is significant in the United States and near significant in Brazil. The results partially validate the study by Mamonov and Benbunan-Fich[59] who found that computer users are more careful of exposing private information when they have knowledge of security breaches.

Conclusion

The literature suggests that culture plays an important role in telemedicine adoption. In order to address this important issue, this research first posited a theory-based comprehensive model to explain factors affecting telemedicine adoption. The model was derived by combining elements from PMT, RDT, TOC, and CAT. The model was then empirically validated using data collected from the United States and Brazil. The results from the SEM-based data analysis showed that culture does not play an important or direct role in telemedicine adoption in the United States or Brazil. Culture, however, indirectly influences telemedicine adoption in the United States and Brazil through information policy. This means that 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.

It should also be noted that the empirical results show information security nearly influences telemedicine adoption in the United States, but not in Brazil. This suggests that even though security standards are essential to telemedicine adoption, health professionals do not consider it as a barrier.

The empirical results show that information policy affects adoption of telemedicine in the United States. This implies that information policies must be carefully reviewed before a decision is made for telemedicine adoption.

The results of this research reveal that information privacy does not significantly impact adoption of telemedicine in either of the two countries. This is an interesting finding, but it may just mean that the users believe that the benefits of telemedicine outweigh the risk of violating patient privacy.

Limitations and suggestions for future research

The limitations of this study are discussed in this section. One limitation is due to the difficulty in gathering the data, especially in the countries studied. Unwillingness to respond to a research survey was one of the biggest obstacles in collecting data. Many individuals did not fill out the online survey sent out to them and the request had to be made in person. Also, in Brazil, collecting data was very difficult because healthcare professionals did not want to take time to complete the survey, which resulted in a smaller sample size for this country. A larger sample could increase the validity of this dissertation's results.

Another limitation was in contacting and convincing the physicians in the United States to participate. In the United States, most physicians were too busy to fill out the survey. A greater proportion of nurses were, therefore, included in the dissertation sample. In Brazil, due to unavailability, physicians were excluded from the sample.

Another limitation of this study is that it cannot be generalized to all countries, but it can be safely stated that before telemedicine is adopted, authorities must pay close attention to telemedicine policies, since these significantly and directly impact information security, privacy, and telemedicine adoption in both countries. In the future, the authors will conduct a research study based on a pairwise comparison of data collected from the United States and Brazil.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Parand Mansouri Rad https://orcid.org/0000-0001-8245-5620

Supplemental material

Supplemental material for this article is available online.

References

1. Hajli N. Developing online health communities through digital media. *Int J Inform Manage* 2014; 34: 311–314.
2. Adewale SO. An internet-based telemedicine system in Nigeria. *Int J Inform Manage* 2004; 24: 221–234.
3. American Telemedicine Association, 2013, http://www.americantelemed.org
4. Bonder S and Zajtchuk R. Changing the paradigm for telemedicine development and evaluation: a prospective model-based approach. *Socio Econ Plan Sci* 1997; 31(4): 257–280.

5. Chaudhry SI, Philips CO, Stewart SS, et al. Telemonitoring for patients with chronic heart failure: a systematic review. *J Card Fail* 2007; 13(1): 56–62.
6. Beaudry B and Pinsonneault A. Understanding user responses to information technology: a coping model of user adaptation. *MIS Quart* 2005; 29: 493–524.
7. Dünnebeil S, Sunyaev A, Blohm I, et al. Determinants of physicians' technology acceptance for e-health in ambulatory care. *Int J Med Inform* 2012; 81: 746–760.
8. Chang J, Chen L and Chang C. Perspectives and expectations for telemedicine opportunities from families of nursing home residents and caregivers in nursing homes. *Int J Med Inform* 2009; 78: 494–502.
9. Ekeland AG, Bowes A and Flottorp S. Effectiveness of telemedicine: a systematic review of reviews. *Int J Med Inform* 2010; 79: 736–771.
10. Barlow J, Bayer S and Curry R. Implementing complex innovations in fluid multi-stakeholder environments: experiences of "telecare." *Technovation* 2006; 26: 396–406.
11. Saliba V, Legido-Quigley H, Hallik R, et al. Telemedicine across borders: a systematic review of factors that hinder or support implementation. *Int J Med Inform* 2012; 81: 793–809.
12. LeRouge C and Garfield M. Crossing the telemedicine chasm: have the U.S. barriers to widespread adoption of telemedicine been significantly reduced? *Int J Env Res Pub He* 2013; 10(12): 6472–6484.
13. Chau PY and Hu PJ. Investigating healthcare professionals' decisions to accept telemedicine technology: an empirical test of competing theories. *Inform Manage* 2002; 39: 297–311.
14. Tarakci H, Ozdemir Z and Sharafali M. On the staffing policy and technology investment in a specialty hospital offering telemedicine. *Decis Support Syst* 2009; 46: 468–480.
15. Hendy J and Barlow J. The role of the organizational champion in achieving health system change. *Soc Sci Med* 2012; 74: 348–355.
16. Adelakun O. Technical factors in telemedicine adoption in extreme resource-poor countries. In: Olivier M and Croteau-Chonka C (eds) *Global health and volunteering beyond borders*. Cham: Springer, 2019, pp. 83–101.
17. Kifle M, Mbarika V, Tsuma C, et al. A telemedicine transfer model for Sub-Saharan Africa. In: *Proceedings of the 41st Hawaii international conference on system sciences*, Waikoloa, HI, 7–10 January 2008.
18. World Health Organization. *Telemedicine: opportunities and developments in member states: report on the second global survey on eHealth* (Global observatory for eHealth series). Geneva: World Health Organization, 2009.
19. Dinesen B, Nonecke B, Lindeman D, et al. Personalized telehealth in the future: a global research agenda. *J Med Internet Res* 2016; 18(3): e53.
20. Berwick D, Nolan T and Whittington J. The triple aim: care, health, and cost. *Health Aff* 2008; 27(3): 759–769.
21. Statista. Internet usage in Brazil—statistics & facts, 2019, https://www.statista.com/topics/2045/internet-usage-in-brazil/
22. United Nations. *World economic situation and prospects*. New York: United Nations, 2019.
23. Combi C, Pozzani G and Pozzi G. Telemedicine for developing countries. A survey and some design issues. *Appl Clin Inform* 2016; 7(4): 1025–1050.
24. Ranganathan C and Balaji S. Key factors affecting the adoption of telemedicine by ambulatory clinics: insights from a statewide survey. *Telemed J E Health* 2020; 26(2): 218–225.
25. Adler-Milstein J, Kvedar J and Bates D. Telehealth among US hospitals: several factors, including state reimbursement and licensure policies, influence adoption. *Health Aff* 2014; 33: 207–215.
26. Baltzan P. *Business driven information systems*. New York: McGraw-Hill, 2019.
27. Barlow J, Singh D, Bayer S, et al. A systematic review of the benefits of home telecare for frail elderly people and those with long-term conditions. *J Telemed Telecare* 2007; 13: 172–179.
28. Kim P and Falcone R. The use of telemedicine in the care of the pediatric trauma patient. *Semin Pediatr Surg* 2017; 26: 47–53.
29. D'Arcy J, Hovav A and Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inform Syst Res* 2009; 20(1): 79–98.

30. Demiris G. The diffusion of virtual communities in health care: concepts and challenges. *Patient Educ Couns* 2006; 62(2): 178–188.
31. Ali Z, Hossain SM, Muhammad G, et al. New zero-watermarking algorithm using hurst exponent for protection of privacy in telemedicine. *IEEE Access* 2018; 6: 7930–7940.
32. Brender J, Nohr C and McNair P. Research needs and priorities in health informatics. *Int J Med Inform* 2000; 58(59): 257–289.
33. Health Insurance Portability and Accountability Act, 2006, https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA
34. LeRouge C, Garfield M and Collins R. Telemedicine: technology mediated service relationship, encounter, or something else? *Int J Med Inform* 2012; 81: 622–636.
35. Kappos A and Rivard S. A three-perspective model of culture, information systems, and their development and use. *MIS Quart* 2008; 32(3): 601–634.
36. Hofstede G. *Culture's consequences: comparing values, behaviors, institutions, and organizations across nations*. New York: SAGE, 2001.
37. Rogers R. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo JT and Petty RE (eds) *Social psychophysiology: a source book*. New York: Guildford, 1983, pp. 153–176.
38. Moor J. Towards a theory of privacy in the information age. *Comp Soc* 1997; 273: 27–32.
39. Alfawaz S, Nelson K and Mohannak K. Information security culture: a behaviour compliance conceptual framework. In: *AISC '10 proceedings of the eighth Australasian conference on information security*, Brisbane, QLD, Australia, January 2010, pp. 47–55. New York: Association for Computing Machinery.
40. Ifinedo P. IT security and privacy issues in global financial services institutions: do socio-economic and cultural factors matter? In: *2008 sixth annual conference on privacy, security and trust, Fredericton, NB*, Canada, 1–3 October 2008, pp. 75–84. New York: IEEE.
41. Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. *Comput Secur* 2012; 31: 83–95.
42. Höne K and Eloff J. Information security policy—what do international information security standards say? *Comput Secur* 2002; 21(5): 402–409.
43. Krasnova H and Veltri N. Behind the curtains of privacy calculus on social networking sites. In: *Wirtschaftsinformatik proceedings*, 2011, http://aisel.aisnet.org/wi2011/26
44. Bansal G, Zahedi F and Gefen D. The impact of personal dispositions on privacy and trust in disclosing health information online. In: *Americas conference on information systems*, 2007, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1567&context=amcis2007
45. Jayasnighe D, Crowder R and Wills G. Model for the adoption of telemedicine in Sri Lanka. *SAGE Open* 2016; 6(3). DOI: 10.1177/2158244016668565.
46. Pelletier-Fleury N, Fargeon V, Lanoé J, et al. Transaction costs economics as a conceptual framework for the analysis of barriers to the diffusion of telemedicine. *Health Policy* 1997; 42: 1–14.
47. Pentzaropoulos G and Siakavellas M. The implementation of advanced telecommunications and services in the Greek academic and research environment: main issues and results. *Telecommun Policy* 2001; 25: 185–196.
48. Brinkmann L, Klein A, Ganslandt T, et al. Implementing a data safety and protection concept for a web-based exchange of variable medical image data. *Int Congr Ser* 2005; 1281: 191–195.
49. Bayer R and Colgrove J. Bioterrorism, public health, and the law. *Health Aff* 2002; 21: 98–101.
50. Fernando J and Dawson L. The health information system security threat lifecycle: an informatics theory. *Int J Med Inform* 2009; 78: 815–826.
51. Kruse C, Smith B, Vanderlinden H, et al. Security techniques for the electronic health records. *J Med Syst* 2017; 41: 127.
52. Damschroder L, Pritts J, Neblo M, et al. Patients, privacy and trust: patients' willingness to allow researchers to access their medical records. *Soc Sci Med* 2007; 64: 223–235.
53. Nunnally J. *Introduction to psychological measurement*. New York: McGraw-Hill, 1970.
54. Hais J, Anderson R, Tatham R, et al. *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall, 1998.

55. Campbell TD and Fiske WD. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychol Bull* 1959; 56(2): 81–105.
56. Swanson R and Holton E. *Research in organizations: foundations and methods of inquiry*. San Francisco, CA: Berrett-Koehler Publishers, 2005.
57. Kruse C, Karem P, Shifflett K, et al. Evaluating barriers to adopting telemedicine worldwide: a systematic review. *J Telemed Telecare* 2018; 24(1): 4–12.
58. Nikkhah H and Sabherwal R. A privacy-security model of mobile cloud computing applications. In: *International conference on information systems (ICIS)*, 2017, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1110&context=icis2017
59. Mamonov S and Benbunan-Fich R. The impact of information security threat awareness on privacy-protective behaviors. *Comput Hum Behav* 2018; 83: 32–44.