

Distance Healthcare in Taiwan

Parand Mansouri Rad*

California State University, Chico, Chico, California, USA

Dalen Chiang

California State University, Chico, Chico, California, USA

James Connolly

California State University, Chico, Chico, California, USA

Adam Mahmood

University of Texas, El Paso, El Paso, Texas, USA

Due to the COVID-19 pandemic, social distancing and quarantine have accelerated the use of distance healthcare to continue caring for patients in Taiwan. However, digitally transferring patients' data increases concern for information privacy and security violations and exposes patients to privacy and security implications. Therefore, the authors investigate the risks of using distance healthcare in Taiwan.

* Corresponding Author. E-mail address: pmansouri-rad@csuchico.edu

I. INTRODUCTION

The coronavirus disease 2019 (COVID-19) pandemic is transforming healthcare more than any other crisis in modern history. Globally, as of January 2022, there have been more than 317 million confirmed cases of COVID-19, including 5.51 million deaths, reported to the World Health Organization. The United States of America (USA) has more than 63 million confirmed cases and more than 844 thousand deaths, while Taiwan has 17,559 confirmed cases and 850 deaths. Taiwan was thought to be highly infected with COVID-19 since the emergence of the virus in China in 2019, as it is less than 100 miles away from China. However, Taiwan's rapid

implementation of disease prevention measures such as rapid tests, patient isolation, a strong public health network, and advanced information technology helped control the disease.

Due to the COVID-19 pandemic, social distancing and quarantine have accelerated the use of distance healthcare to continue caring for patients. However, transferring patients' data digitally increases concern for information privacy and security violations and exposes patients to privacy and security implications (Parimbelli et al., 2018). Therefore, the authors investigate risks involved in using distance healthcare in Taiwan by adopting Mansouri-Rad, Mahmood, Putnam, and Thompson's (2017) model.

According to the International Monetary Fund, Taiwan is an advanced economy with a per capita GDP (PPP \$52.960 in 2018), ranking as the world's 19th largest economy. Taiwan has a single-payer system, which means that the government controls healthcare payments, yet most healthcare providers and hospitals are privatized. Taiwan has a population of about 23.58 million in a 13,890 square mile land, which contains many mountains and isolated islands (Wikipedia, 2021) with rural areas that would benefit from implementing distance healthcare. Since the pandemic, Taiwan has extended its electronic healthcare, and hospitals use more online medical records to fight the COVID-19 outbreak.

Since there has been a significant increase in using distance healthcare in Taiwan (Drees, 2020), this research aims to identify the risks associated with the implementation of distance healthcare in Taiwan. The authors examine the impact of information security, privacy, and policies in distance healthcare implementation in Taiwan. The researchers collected data by surveying physicians, nurse practitioners, executives, and information technology specialists from Taiwan. The authors compare the results with the study by Mansouri-Rad, Mahmood, Putnam, and Thompson (2017).

II. PREVIOUS WORK

Since the start of COVID-19, the use of distance healthcare has increased significantly but has come with an increase in security, privacy, and policy concerns. Since the pandemic and with the increase of apps, texts, and internet use, more healthcare professionals are using distance healthcare (Kim and Falcone, 2017) and developing more concerns about the security of patients' information. The secure transmission of electronic medical records (EMRs) is still a crucial risk in distance healthcare implementation. An EMR contains private data, must be transferred with high

security and should be available only to authorized healthcare professionals. Therefore, it is essential to ensure that security procedures are correctly followed in online consultations, including sending audio and pictures and keeping recorded videos and medical documents (Li, Bai, and Zaman, 2013).

Yuksel et al. (2017) systematically studied research papers with a method-based approach and provided a comprehensive survey of cryptographic approaches of electronic health services (EHS) to demonstrate that using distance healthcare increases information security, authentication, and authorization risks. When patients' health information is shared with health and human services, hospitals and physicians, authentication must be accomplished in all steps and levels. In addition, Jnr (2020) used the Preferred Reporting Items for Systematic Reviews (PRISMA) to review 35 distance healthcare research studies between 2019 and May 2020. Information security was one of the obstacles in using distance healthcare and causing risks during virtual visit appointments via Zoom. In another study, Xhafa, Li, Zhao, Li, Chen, and Wong (2015) also revealed that patients are concerned about security and unauthorized access to sensitive data in cloud-based health systems.

In addition to security risks, privacy and integrity of healthcare data can also be problematic in using electronic health systems. According to Gope and Hwang (2016), patients' privacy is more vulnerable when health professionals consider adopting distance healthcare. The authors discussed the development of the Internet of Things in modern healthcare. They revealed that data privacy is the most important risk in using the body sensor network technology since it could leak patients' vital information to external or neighboring networks. Dinesen et al. (2016) focused on privacy and confidentiality in assessing e-diaries used to communicate with health care professionals' in-home rehabilitation programs for diabetes. The

authors identified confidentiality, integrity, availability, and quality as threats to patients' information. Moreover, they argued that distance healthcare at home offers more risks and threats to patient health information privacy and confidentiality than hospitals and healthcare organizations. Therefore, their study suggests a need to develop adequate levels of information privacy to support the rapid implementation of new telehealth technologies.

During the COVID-19 pandemic, there have been temporary modifications in the USA's Health Insurance Portability and Accountability Act (HIPAA) and reimbursement policies. In Taiwan, during COVID-19, telehealth is improving rapidly under the National Health Insurance system, and there is a need to protect the patients and their privacy. There are a variety of regulations, such as the Personal Information Protection Act, the Physician Act, and the Medical Care Act, that oversee the proper use of personal information. However, Taiwan still lacks a single centralized standard such as Health Insurance Portability and Accountability Act in the USA (Yang, Lin, Chang, and Jian, 2006). Government policies are extremely influential in the diffusion of technology, especially where governments control most of the regulations (Kifle, Mbarika, Tsuma, Wilkerson, and Tan, 2008). Policies can also improve reimbursement plans to reduce health care costs (Ranganathan and Balaji, 2019) and provide guidelines for using technology in distance healthcare.

Hofstede (1991) defined culture as the collective mindset distinguishing the members of one nation from another and described it as "the collective programming of the mind distinguishing the members of one group or category of people from another" (p. 5). Hofstede's original model includes four dimensions: individualism (IND), power distance (PDI), uncertainty avoidance (UAI), and masculinity (MAS). The IND is the degree to which individuals are integrated into groups. The PDI refers to the degree of inequality

between a less powerful individual and a more powerful one. MAS is the distribution of roles between the genders. The UAI measures the extent to which a society feels threatened by uncertainty and tries to avoid these situations.

Organizational culture can influence technology innovation and implementation (Gruenhagen and Parker, 2020). Chung, Thompson, Joe, Hall, and Demiris (2017) examined the diffusion of technology among Korean and Korean-American older adults. The authors used interviews and focus groups and found that culture plays an important role in using home-based monitoring technology. The Korean group was more enthusiastic about using electronic health devices than the Korean-American group. Despite some participants being concerned about privacy risks, they were still interested in using the device.

Moreover, Latifi and Alizadeh (2016) surveyed chief information officers to investigate the national factors influencing adopting distance healthcare. The authors did not find any significant relationship between cultural factors and distance healthcare implementation. In this research paper, the authors further investigate the impact of culture on distance healthcare implementation in Taiwan and compare the results with the study by Mansouri-Rad, Mahmood, Putnam, and Thompson (2017), which investigated the relationship between culture and telemedicine in the USA.

III. THEORIES AND RESEARCH MODEL

The model is adopted from Mansouri-Rad, Mahmood, Putnam, and Thompson (2017) and uses multiple theories (i.e., theory integration) to measure the risk of information security, privacy, policy, and culture in distance healthcare implementation (Fig. 1). The theories are protection motivation theory (PMT; Rogers, Cacioppo, and Petty, 1983), rational deterrence theory (RDT; Beccaria, 1963),

control access theory (CAT; Moor, 1997), and the theory of culture (TOC; Hofstede, 2001).

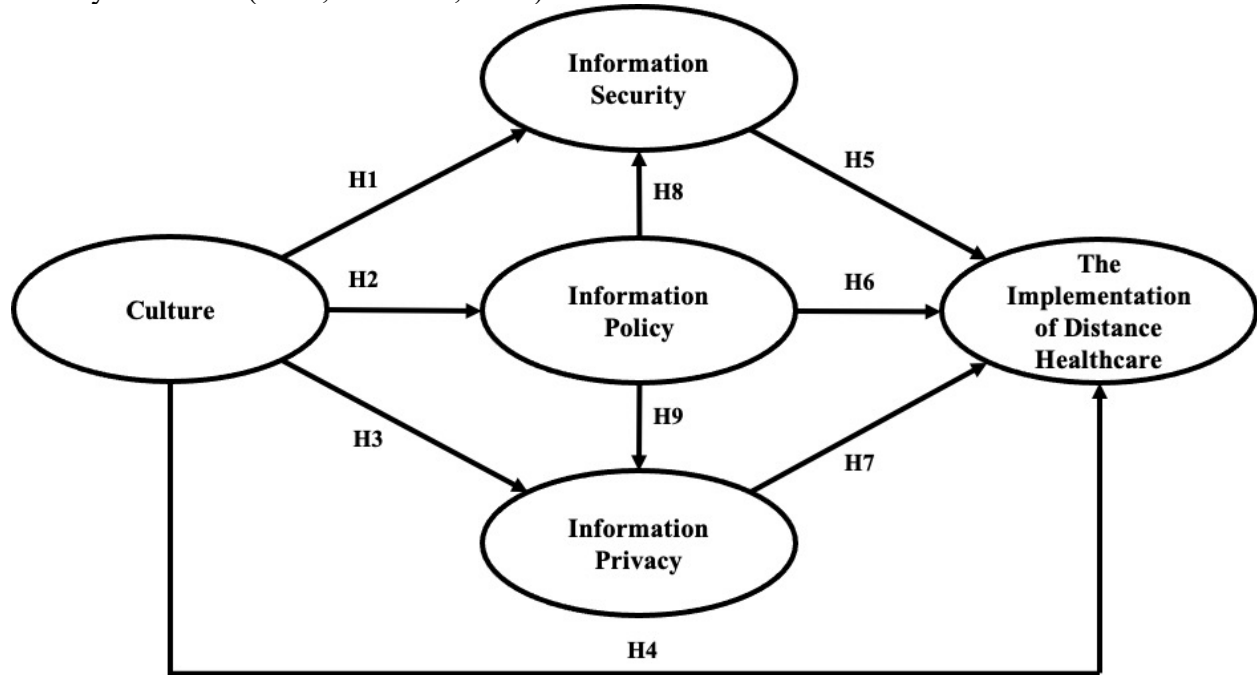


FIGURE 1. RISKS IN DISTANCE HEALTHCARE IMPLEMENTATION MODEL.

The PMT explains the effects of fear appeals to motivate people to avoid harmful health behavior (Rogers, 1983). Threat appraisal is the process of assessing a person's fear perception of how threatened they feel when facing a certain situation. In this paper, preventing security breaches in healthcare will have a positive impact on implementing distance healthcare.

According to Moor's (1997) CAT, individuals have privacy when they are secured from intrusion and information access by others. In the context of this study, protecting patients' information privacy will have a positive effect on implementing distance healthcare.

The RDT expresses the behavior of a person to control or prevent punishment. In the context of patients' health information, implementing rules and regulations will prevent criminals from misusing patients' information.

Hofstede's (2001) TOC includes a framework to distinguish countries based on their culture and differentiate each country based on how they conduct business.

3.1. Hypotheses

The results of this study are compared with the study by Mansouri-Rad, Mahmood, Putnam, and Thompson (2017), which investigated the relationship between culture and telemedicine in the USA. The reason for this comparison is that according to Hofstede's (2001) cultural indices, there is a major difference between Taiwan and the USA regarding individualism-collectivism (17 versus 91). There is also a substantial variance in the respective Hofstede index values for uncertainty avoidance with (69 for Taiwan versus 46 for the US). In terms of power distance, Taiwan has a higher score (58), whereas the USA has a moderate score (44).

Lastly, regarding masculinity, Taiwan has a medium to low MAS culture (45) versus the USA (62).

The U.S. Department of Health and Human Services (HHS) defines information security as follows: "Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of information." (HHS, p. 4)

Chen and Zahedi (2016) analyzed the user's security behaviors in the USA and China using 718 collected surveys. The authors found that a significant difference exists between the two cultures in the way they protect their information security, pursue assistance, and avoid security threats. Further, Chen and Zahedi discovered that Hofstede's collectivism and power distance has a moderating impact on perceptions of information security threat and coping abilities between two countries. Based on the above studies and in comparison with Mansouri-Rad, Mahmood, Putnam, and Thompson (2017), which found no significant impact of culture on information security in the USA, this study hypothesizes that:

H₁: National culture traits positively impact health information security in Taiwan.

Flores, Antonsen, and Ekstedt (2014) investigated the role of national culture on information security knowledge sharing and security policies. The authors studied the difference between the American (i.e., more individualist and masculine culture) and Swedish (i.e., less individualist, feminine country) organizations. The result of structural equation modeling disclosed that there is a significant distinction between the cultures. The study revealed that the companies in the USA, unlike the Swedish companies, enforce their visible information security policies and control their employees.

According to Cockcroft and Rekker (2015), national culture impacts each country's

regulation of information privacy. The authors found that Asian countries tend to care less about information privacy policies and value family and friendship more. They also showed that such countries do not prioritize the right to be left alone. However, Asian countries put greater trust in their government and trust that they are able to protect their privacy with their regulations (Cockcroft and Rekker, 2015). Based on the above studies and in comparison with Mansouri-Rad, Mahmood, Putnam, and Thompson (2017), which found a positive and significant impact of culture on information policy in the USA, this study hypothesizes that:

H₂: National culture traits positively impact health information policy in Taiwan.

Miltgen and Peyrat-Guillard (2014) studied the impact of national culture on Europeans' decisions to protect their data privacy. Using focus groups, the authors found that individuals from all countries expressed their concern with their information privacy; however, south Europeans have a choice while the eastern Europeans are required to disclose.

Omrani and Soulie (2017) investigated people's concerns on online privacy among different cultures in Europe. Their results revealed that countries with higher power distance and masculinity and lower uncertainty avoidance index are more concerned about their privacy. According to (Milberg, Smith, & Burke, 2000), individualism positively impacts information privacy concerns. Individualist societies appreciate their private life and independence from others. Individualist societies are more concerned with disclosing their personal information. Individuals in individualistic societies are more likely to be concerned about potential privacy intrusion and hesitant to disclose personal information (Miltgen & Peyrat-Guillard, 2014). On the other hand, in Taiwan, a collectivist society, people are less sensitive to privacy concerns (Mohammed and Tejay, 2017) and are more likely to trust organizations with their personal

information. In this research paper, the authors hypothesize:

H₃: National culture traits positively impact health information privacy in Taiwan.

National culture has a strong impact on individuals and organizations (Leidner and Kayworth, 2006). Many cultural studies reviewed by Leidner and Kayworth (2006) revealed that cultures with higher uncertainty avoidance are more resistant to the implementation of information technology. The UAI is the degree to which a society feels threatened by uncertainty. It explains society's response to ambiguity. Nations with a high degree in UA believe in guidelines and laws. Societies with a lower degree in UA show more tolerance for unknown situations and are more open-minded about new ideas. These societies believe that it is fine to question the people in higher authorities.

In Taiwan, distance healthcare is provided through the government, and individuals accept it when it is encouraged or forced to use by the authorities. Mohammed and Tejay (2017) used the data collected from Trinidad and Tobago and determined that culture plays a major factor in people's decision to adopt technology and interact online. Hoque and Bao (2015) investigated the impact of culture as defined by Hofstede on the adoption of e-health in Bangladesh surveying private and public hospitals. The result of SEM showed that masculinity and power distance impacts intention to use e-health. Based on the above studies, and in comparison with (Mansouri-Rad, Mahmood, Putnam, and Thompson (2017), the authors hypothesize:

H₄: National culture traits positively impact distance healthcare implementation in Taiwan.

Information security is necessary to guarantee that technology infrastructure delivers healthcare in a safe and effective manner. Jnr (2020), Kim and Falcone (2017), Yuksel, Kupcu, and Ozkasap (2017), and Xhafa, Li, Zhao, Lii, Chen, and Wong (2015)

demonstrated that the concern about patient information security and access control could compromise the implementation of distance healthcare. Thus, the authors hypothesize the following:

H₅: Health information security impacts distance healthcare implementation in Taiwan.

Patients' information policy such as HIPAA determines some standards of roles and responsibilities that are essential to distance healthcare implementation. Policies can also improve reimbursement plans to reduce health care costs (Ranganathan and Balaji, 2019). In Taiwan, the privacy of medical information can be protected by the Taiwan government's guidelines and, therefore, encourage physicians to adopt telehealth to their practices (Yang, Lin, Chang, and Jian, 2006). Thus, the authors hypothesize:

H₆: Health information policies impact distance healthcare implementation in Taiwan.

Healthcare data privacy and integrity can also be problematic in using electronic health systems. According to Gope and Hwang (2016), Dinesen et al. (2016), Dünnebeil, Sunyaev, Blohm, Leimeister, and Krcmar (2012), and Ali, Hossain, Muhammad, and Aslam (2018), patient privacy is more vulnerable when health professionals consider adopting distance healthcare. Patients' information privacy is still named a barrier to telehealth implementation by non-adopters. This is not surprising since Cheung and Ripley (2021) reported that Taiwan's government's systems face between 20 million to 40 million cyberattacks every month. Therefore, the authors hypothesize:

H₇: Privacy of health information impacts distance healthcare implementation in Taiwan.

Taiwan has many regulations, such as Physician Act, Personal Information Protection Act (PIPA), and the Electronic Signature Act, to protect people's electronic data. However, the Department of Health needs a single regulation system such as HIPAA to pay close attention to

managing EMRs. Government policies are crucial in Taiwan, where the government controls most of the healthcare system and oversees the implementation and use of e-health by private organizations (Kifle, Mbarika, Tsuma, Wilkerson, and Tan, 2008). Thus, the authors hypothesize:

H₈: Health information policy impacts information security.

H₉: Health information policy impacts information privacy.

IV. METHODOLOGICAL PROCEDURES

The authors used the survey instrument based on the model in Fig. 1, which was adopted from Mansouri-Rad, Mahmood, Putnam, and Thompson (2017) in Taiwan. There are 49 questions in the instrument. Twenty-four questions cover information security, privacy, policy, and telemedicine adoption, 20 questions include Hofstede’s culture dimensions, and the remaining items provide demographic information. The instrument for collecting data

was translated from English into Chinese, and 600 questionnaires were then distributed in clinics, medical centers, metropolitan hospitals, and community hospitals. Of the total 474 responses the authors received, 433 were usable. Forty percent of the respondents in Taiwan were males, while 60% were females; 27% were physicians, 40% were nurse practitioners, 17% were executives, 7% were information technology specialists, and 10% were others. The authors chose Taiwan for convenience because of the type of healthcare system and the fact that it is at a different stage in implementing distance healthcare. Taiwan has a single-payer system, and the government controls healthcare. In comparison, the USA’s health care system is the most expensive and unique among advanced industrialized countries and the world. Health care facilities are largely owned and operated by private sector businesses. Only recently did the USA enact legislation to mandate healthcare coverage for almost everyone.

TABLE 1. SCALE DEVELOPMENT.

Construct (N° of items)	Mean, Std. Dev., Cronbach Alpha	Factor Loadings	Var. Extracted
Culture (20)	102.66, 10.885, .813	.84, .84, .86, .89, .87, .80, .81, .61, .70, .47, .46, .33, .11, .04, .31, -.13, .19, .06, -.26, -.03	.81
Implementation (5)	27.82, 4.484, .842	.53, .61, .66, .91, .88	.20
Privacy (4)	25.23, 3.058, .902	.88, .89, .82, .77	.09
Information Security (5)	30.36, 3.783, .92	.81, .86, .84, .88, .83	.14
Policy (5)	29.41, 4.085, .918	.84, .84, .79, .88, .85	.17

4.1. Reliability and Validity

Cronbach’s alpha was first used to determine the reliability of the constructs (Table 1). The Cronbach alpha analysis values are

high, showing a reliable questionnaire. Implementation, information privacy, information security, and information policy have reliability scores of 0.84, 0.90, 0.92, and 0.92, respectively. The results meet Nunnally's (1970) standards denoting that 0.70 is an acceptable level of reliability for a construct.

Convergent validity and discriminant validity were determined by calculating factor loadings and computing the correlations between all validated constructs. All five items in the information security, privacy, policy, and the implementation group, loaded very well (\geq

0.40). The average variance explained by each factor the researchers obtained from factor analysis communalities for Taiwan is 0.09, 0.14, 0.17, and 0.20 for privacy, security, policy, and implementation, respectively.

4.2. Correlation Analysis

Table 2 provides the results of a correlation test to understand the influence among implementation and the dependent variables.

TABLE 2. CORRELATION ANALYSIS.

Constructs	Culture	Policy	Privacy	Security	Implementation
Culture	1.00				
Policy	0.46***	1.00			
Privacy	0.44***	0.48***	1.00		
Security	0.38***	0.60***	0.31*	1.00	
Implementation	0.42***	0.74***	.44***	.51***	1.00

* Significant at the .10 level
** Significant at the .05 level
*** Significant at the .01 level.

Table 2 shows correlations among constructs for Taiwan. The discriminant validity was assessed, and correlations among items within the information security, privacy, policies, and distance healthcare constructs were greater than .66, .58, .62, and .36, respectively ($p < .05$). All correlations among constructs are significant.

4.3. Structural Equation Modeling

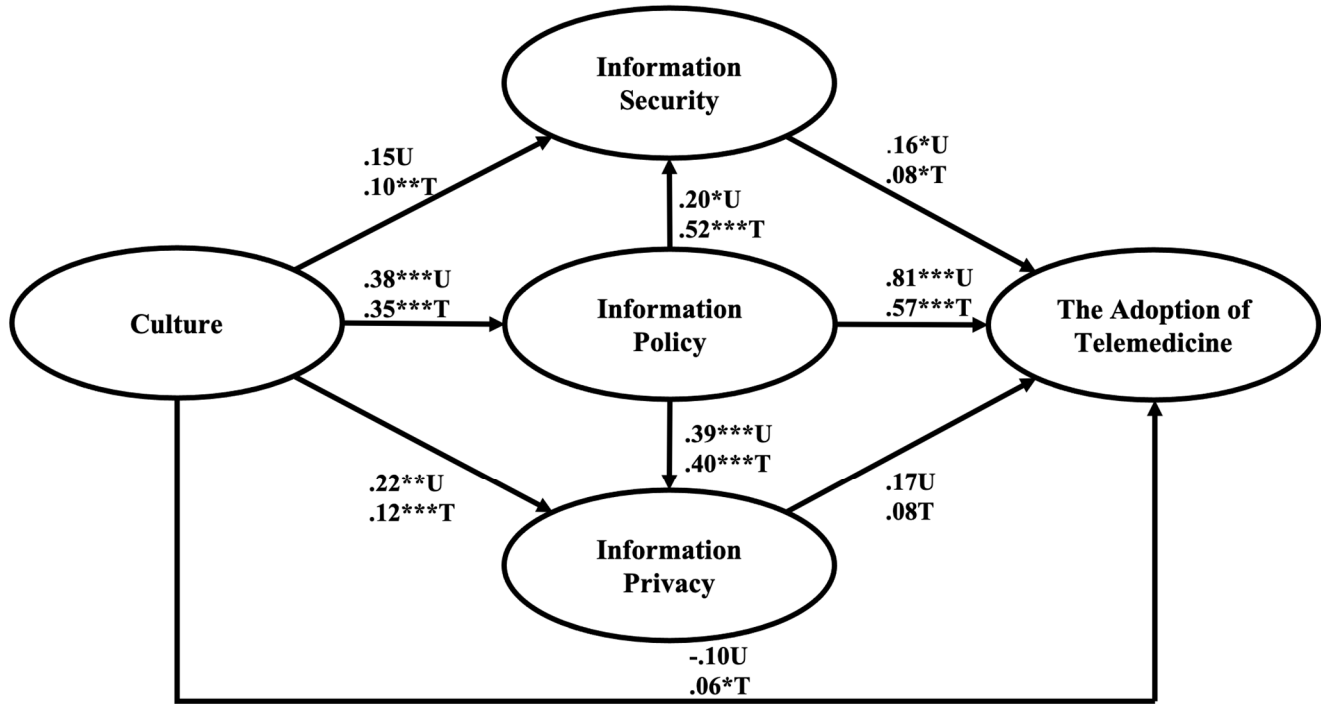
Fig. 2 shows the result for the hypothesized model for Taiwan and compares them with the USA data from Mansouri-Rad, Mahmood, Putnam, and Thompson (2017). Fig. 2 shows the hypothesized model for the USA and Taiwan. The AMOS/SEM results reveal that the path coefficient from culture to information security (H1) is only significant for

Taiwan at the .05 level. The path coefficient from culture to information policy (H2) is significant for both countries at the .01 level. The results also indicate that the path coefficient from culture to information privacy (H3) is significant at the .05 level or lower for the USA and Taiwan. The results further reveal that Taiwan has a significant path coefficient from culture to telemedicine adoption (H4) at the .10 level.

Moreover, the path coefficient from information security to distance healthcare implementation (H5) is significant at the .10 level. There is a significant path coefficient from information policy to distance healthcare implementation (H6) at the .01 level. There is no significant path coefficient from information privacy to distance healthcare implementation (H7) in the US, but in Taiwan, this path is

significant at the .10 level. The path coefficients from information policy to information security (H8) are significant in both countries at the .01 level. The path coefficient from information policy to information privacy (H9) is significant

at the .01 level for the USA but not for Taiwan. The path coefficient from information security to information privacy is significant at the .01 level for both countries.



* Significant at the .10 level, ** Significant at the .05 level *** Significant at the .01 level

FIGURE 2. RESULTS FROM THE HYPOTHESIZED MODEL.

TABLE 3: MULTIPLE COMPARISONS.

Dependent Variable	(I) Country	(J) Country	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Security	Taiwan	USA	-1.2831*	.40501	.005	-2.2342	-.3319
	USA	Taiwan	1.2831*	.40501	.005	.3319	2.2342
Privacy	Taiwan	USA	-.2850	.39775	.754	-1.2191	.6492
	USA	Taiwan	.2850	.39775	.754	-.6492	1.2191
Policy	Taiwan	USA	1.0996*	.41067	.021	.1352	2.0641
	USA	Taiwan	-1.0996*	.41067	.021	-2.0641	-.1352
Distance healthcare	Taiwan	USA	-2.5899*	.39848	.000	-3.5257	-1.6540
	USA	Taiwan	2.5899*	.39848	.000	1.6540	3.5257
Culture	Taiwan	USA	10.6341*	.93829	.000	8.4305	12.8377
	USA	Taiwan	-10.6341*	.93829	.000	-12.8377	-8.4305

Based on observed means.

The error term is Mean Square (Error) = 113.683.

*. The mean difference is significant at the .05 level.

Table 3 shows that mean scores for security were statistically significantly different between Taiwan and the USA ($p < .01$). Mean scores in privacy were not significantly different between the USA and Taiwan ($p = .285$). Mean scores in policy were statistically different between Taiwan and the USA ($p < .05$). Mean for distance healthcare implementation were statistically different between Taiwan and the USA ($p < .0005$). Mean culture was statistically significantly different between Taiwan and USA ($p < .0005$).

V. DISCUSSION

This research empirically validates H1, which suggests that culture impacts information security in Taiwan. Culture does not have an impact on information security in the USA. A significant difference between American and Chinese cultures is how they protect their information security, pursue assistance, and avoid security threats. The multiple comparisons tests indicate a significant difference in security between Taiwan and the USA ($p = .005$; see Table 7.3).

This study shows that culture has a positive and significant impact in both countries on information policy. This means the findings align with Flores, Antonsen, and Ekstedt (2014) and Cockcroft and Rekker (2015), who believed that national culture impacts each country's regulation of information privacy. Taiwan's telemedicine policies are regulated through the government and are aligned with Taiwan's culture. The results of this research suggest that culture affects information privacy in Taiwan and USA. The study also aligns with Miltgen and Peyrat-Guillard (2014), who found that culture impacts how individuals in different cultures express their concern with their information privacy. Omrani and Soulie (2017) also revealed that countries with higher power distance and masculinity index are more concerned about their privacy, and countries

with higher uncertainty avoidance index have fewer privacy concerns.

Culture affects distance healthcare implementation directly and significantly, as the authors hypothesized in H4; this finding aligns with the studies by Leidner and Kayworth (2006) and Mohammed and Tejay (2017), who believed culture plays a major factor in people's decision to adopt technology and interact online. Taiwan's culture played an important role in adopting telemedicine and controlling Covid-19 during the pandemic. However, culture did not impact telemedicine in the study by Mansouri-Rad, Mahmood, Putnam, and Thompson (2017).

This research empirically shows that distance healthcare implementation is significantly affected by information security in Taiwan and the USA. The result of this study empirically confirms the findings by Jnr (2020), Kim and Falcone (2017), Yuksel, Kupcu, and Ozkasap (2017), and Xhafa, Li, Zhao, Li, Chen, and Wong (2015), according to whom information security can be an obstacle to distance healthcare implementation. In Taiwan, data protection is mainly governed by the Personal Data Protection Act of 2015, and they have been successful in using telehealth for disease control since 2020.

The results of this research show that the information policies significantly and positively impact distance healthcare implementation in both countries. The findings are also aligned with Ranganathan and Balaji's (2019) and Yang, Lin, Chang, and Jian's (2006) studies. In Taiwan, government policies are extremely influential in the diffusion of technology and control most regulations. During Covid, Taiwan's government made telemedicine available to patients in quarantine and allowed national health insurance to support telemedicine services (Chu, Wang, Lee, Lin, and Feng, 2021).

The results of this research demonstrate that information privacy does not influence the implementation of electronic health in Taiwan

or the USA. The results of this study in Taiwan contradict Gope and Hwang (2016), Dinesen et al. (2016), Dünnebeil, Sunyaev, Blohm, Leimeister, and Kremer (2012), and Ali, Hossain, Muhammad, and Aslam (2018), who considered health information privacy an important factor in implementing electronic health. Taiwan controlled the pandemic by tracking and disclosing patients' health information, and the Taiwanese accepted the invasion of their health information privacy, which seems to have no boundaries.

The results of this research reveal that information policy impacts information security and privacy in both countries. The result is in line with Kifle, Mbarika, Tsuma, Wilerson, and Tan (2008) and Nikkhah and Sabherwal (2017), which showed a relationship between information security and policy. This result demonstrates Taiwanese health professionals need a single robust distance healthcare policy and see information policies as a barrier to the implementation of distance healthcare.

VI. CONCLUSION

The results from the SEM-based data analysis showed that culture plays an important and direct role in distance healthcare implementation in Taiwan. Information policy affects the implementation of distance healthcare. In Taiwan, the combination of culture and implementing the right information policies have played an enormous role in the nation's successful COVID-19 response with using distance healthcare.

Moreover, information security influences distance healthcare implementation. The results show that without information security, practicing distant healthcare is not achievable. The current investigation did not find a significant relationship between information privacy and the implementation of distance healthcare in Taiwan. Taiwan's population trusts their government to gather and disclose their detailed covid information to

overcome the pandemic. Privacy risks have not prevented them from using big data analysis and more technology-advanced healthcare measures. Specifically, culture and information policies have significant dissimilarities in how the two countries controlled the pandemic for the last two years using distance healthcare. Taiwan has improved its distance healthcare since the pandemic has started by implementing more telehealth regulations to protect people's electronic data. Taiwan's government controls most of the healthcare system and oversees the implementation and use of e-health by private organizations. In the USA, telemedicine has improved by loosening electronic health reimbursement and licensure regulations by the government. However, the future of distance healthcare is still in question in the coming years. It is unclear if the government, states, and private payers will continue reimbursing distance healthcare. In addition, the status of temporary telehealth flexibilities, which are tied to the status of the state of emergency declarations, is still in question after the end of the emergency.

6.1. Limitations

Collecting data from health professionals, especially physicians, was the most challenging part of this study; therefore, the authors used a convenience sample rather than a random sample. This study cannot generalize the outcome to broader populations. Moreover, the sample size in this study is smaller than the author intended.

REFERENCES

- Ali, Z., Hossain, S. M., Muhammad, G., & Aslam, M., "New zero-watermarking algorithm using Hurst Exponent for protection of privacy in telemedicine", *IEEE Access*, 6, 2018, 7930–7940.

- Chen, Y., & Zahedi, F., "Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China", *MIS Quarterly*, 40(1), 2016, 205–222.
- Chung, J., Thompson, H., Joe, J., Hall, A., & Demiris, G., "Examining Korean and Korean American older adults' perceived acceptability of home-based monitoring technologies in the context of culture", *Informatics for Health & Social Care*, 42(1), 2017, 61–76.
- Cockcroft, S., & Rekker, S., "The relationship between culture and information privacy policy", *Electron Markets*, 26, 2015, 55–72.
- Dünnebeil, S., Sunyaev, A., Blohm, I., Leimeister, J. M., & Krcmar, H., "Determinants of physicians' technology acceptance for e-health in ambulatory care", *International Journal of Medical Informatics*, 81, 2012, 746–760.
- Demiris, G., "The diffusion of virtual communities in health care: Concepts and challenges", *Patient Education and Counseling*, 62(2), 2006, 178–188.
- Dinesen, B., Nonnecke, B., Lindeman, D., Toft, E., Kidholm, K., Jethwani, K., & Young, H., "Personalized telehealth in the future: A global research agenda", *Journal of Medical Internet Research*, 18(3), 2016.
- Drees, J. *What the US can learn from Taiwan's EHR system and COVID-19 response*. ASC Communications, 2020.
- Flores, W. R., Antonsen, E., & Ekstedt, M., "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture", *Computers & Security*, 43, 2014, 90–110.
- Gope, P., & Hwang, T., "BSN-Care: A secure IoT-based modern healthcare system using body sensor network", *IEEE Sensors Journal*, 16(5), 2016, 1368–1376.
- Govender, S., Kritzger, E., & Loock, M., "The influence of national culture on information security culture", *IIMC International Information Management Corporation*. Durban, South Africa: Paul Cunningham and Miriam Cunningham (Eds), 2016.
- Gruenhagen, J., & Parker, R., "Factors driving or impeding the diffusion and adoption of innovation in mining: A systematic review of the literature", *Resources Policy*, 65, 2020.
- HHS.
<https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf>
HIPAA. (2006).
<https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA>
- Hofstede, G. *Cultures and organizations: Software of the mind*. McGraw-Hill, 1991.
- Hofstede, G. *Culture's Consequences: comparing values, behaviors, institutions, and organizations across nations*. NY: SAGE Publications, 2001.
- Jnr, B. A., "Use of telemedicine and virtual care for remote treatment in response to COVID-19 pandemic", *Journal of Medical Systems*, 44(132), 2020.
- Kifle, M., Mbarika, V., Tsuma, C., Wilkerson, D., & Tan, J. (2008). A TeleMedicine transfer model for sub-Saharan Africa. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*.
- Kim, P., & Falcone, R. "The use of telemedicine in the care of the pediatric trauma patient", *Seminars Pediatric Surgery*, 26, 2017, 47–53.
- Latifi, F., & Alizadeh, S., "The influence of national factors on transferring and adopting telemedicine technology: Perspectives of chief information

- officers”, *International Journal of E-Health and Medical Communications (IJEHMC)*, 7(3), 2016.
- Leidner, D., & Kayworth, T., “Review: A review of culture in information systems research: Toward a theory of information technology culture conflict”, *MIS Quarterly*, 30(2), 2006, 357–399.
- Li, J., Bai, Y., & Zaman, N., “A fuzzy modeling approach for risk-based access control in eHealth cloud”, *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. Melbourne: IEEE, 2013.
- Luciano, E., Mahmood, A., & Mansouri Rad, P. (2020). Telemedicine adoption issues in the United States and Brazil: Perception of healthcare professionals. *Health Informatics Journal*, 26(4), 2344-2361.
- Mansouri-Rad, P., Mahmood, A., Putnam, K., & Thompson, S., “Oil and gas exploration and telemedicine: Culture factors in telemedicine adoption”, *Oil, Gas & Energy Quarterly*, 2017.
- Miltgen, C., & Peyrat-Guillard, D., “Cultural and generational influences on privacy concerns: a qualitative study in seven European countries”, *European Journal of Information Systems*, 23(2), 2014, 103–125.
- Mohammed, Z., & Tejay, G., “Examining privacy concerns and ecommerce adoption in developing countries: The impact of culture in shaping individuals’ perceptions toward technology”, *Computers & Security*, 67, 2017, 254–265.
- Moor, J., “Towards a theory of privacy in the information age”, *Computers and Society*, 273, 1997, 27–32.
- Nikkhah, H., & Sabherwal, R., A privacy-security model of mobile cloud computing applications. *International Conference on Information Systems (ICIS)*, 2017.
- Nunnally, J., *Introduction to psychological measurement*. McGraw-Hill, 1970.
- Oh., P., & Jo, K., “Current status and progress of telemedicine in Korea and other countries”, *Healthcare Informatics Research*, 21(4), 2015, 239–243.
- Omrani, N., & Soulie, N., “Culture, privacy conception and privacy concern: Evidence from Europe before PRISM”, *Asia-Pacific Regional Conference of the International Telecommunications Society (ITS)*. Kyoto, Japan: International Telecommunications Society (ITS), 2017.
- Parimbelli, E., Bottalico, B., Losiouk, E., Tomasi, M., Santosuosso, A., Lanzola, G., . . . Bellazzi, R. “Trusting telemedicine: A discussion on risks, safety, legal implications and liability of involved stakeholders”, *International Journal of Medical Informatics*, 112, 2018, 90–98.
- Ranganathan, C., & Balaji, S., “Key factors affecting the adoption of telemedicine by ambulatory clinics: Insights from a statewide survey”, *Telemedicine and e-Health*, 26(2), 2019, 218–225.
- Rogers, R., Cacioppo J., & Petty, R., “Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation”, In *Social Psychophysiology* (pp. 153–177). Guilford, 1983.
- Ruighaver, A. B., Shanto, S. B., & Chang, C., “Organisational security culture: Extending the end-user perspective”, *Computers & Security*, 26(1), 2007, 56–62.
- Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G., “Security and privacy in the medical Internet of Things: A review”, *Security and Communication Networks*, 2018.

- United Nations, “World economic and social survey: Frontier technologies for sustainable development”, 2018. https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESS2018_ch4_en.pdf
- Van Niekerk, J., & Von Solms, R., “Information security culture: A management perspective. *Computers & Security*”, 29(4), 2010, 476–486.
- Wikipedia*, “Taiwan”, 2021. <https://en.wikipedia.org/wiki/Taiwan>
- World Health Organization, “Telemedicine: Opportunities and developments in member states”, 2010. https://www.who.int/goe/publications/goe_telemedicine_2010.pdf
- Xhafa, F., Li, J., Zhao, G., Li, J., Chen, X., & Wong, D., “Designing cloud-based electronic health record system with attribute-based encryption,” *Multimedia Tools and Applications*, 74(10), 2015, 3441–3458.
- Yang, C.-M., Lin, H.-C., Chang, P., & Jian, W.-S., “Taiwan’s perspective on electronic medical records’ security and privacy protection: Lessons learned from HIPAA”, *Computer Methods and Programs in Biomedicine*, 82, 2006, 277–282.
- Yuksel, B., Kupcu, A., & Ozkasap, O., “Research issues for privacy and security of electronic health services”, *Future Generation Computer Systems*, 68, 2017, 1–13.