

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Effect of Health Information Privacy Concerns on Usage of mHealth Apps, Having Trust in mHealth App Security as a Mediator and Higher Authority Support as a Moderator

Muhammad Saad Hussain

MS Healthcare Management, Riphah International University

Saadhussain9110@gmail.com

Myrah khan

MS Healthcare Management, Riphah International University; Manager, Quality Assurance & Infection Control, Islamabad Dental Hospital, Islamabad, Pakistan

myrahkhan12@gmail.com

Dr. Maimuna Iqbal

MS Healthcare Management, Riphah International University

Maimunaiqbal491@gmail.com

Ali Murtaza Turi

MS Healthcare Management, Riphah International University

Ali.moortaza12@gmail.com

Dr. Waqas Saeed

MS Public Health, Health Services Academy, Islamabad

Waqassaeed30@gmail.com

Dr. Muhammad Ali Abbas

MBBS, University of Health Sciences

mohammadaliabbass@gmail.com

ABSTRACT

Purpose: The purpose of this study is to explore the impact of health information privacy concerns on the usage of mHealth apps, with trust in mHealth app security acting as a mediator and higher authority support acting as a moderator.

Design/Methodology: Using a convenience sampling technique, data was collected from 220 staff and patients of various private hospitals in Islamabad and Rawalpindi, Pakistan, through a structured questionnaire. Data analysis was conducted using SPSS to test the hypothesized relationships.

Findings: The results confirmed that health information privacy concerns significantly impact both trust in mHealth app security and the actual usage of mHealth apps. Trust

in mHealth app security was found to mediate the relationship between privacy concerns and app usage. Furthermore, higher authority support moderated the relationship between trust in app security and mHealth app usage such that the relationship strengthened in the presence of higher support.

Significance: While extensive research exists on digital health adoption, limited attention has been given to the combined effect of privacy concerns, security trust, and institutional support. This study offers a unique contribution by empirically validating the mediating role of trust and the moderating effect of higher authority support, especially in a developing country context.

Research limitations: The cross-sectional nature of the study limits causal inference. The use of convenience sampling may result in selection bias and limit the generalizability of results. Furthermore, relying solely on quantitative methods restricts the exploration of in-depth user perspectives. Future research should adopt longitudinal or qualitative designs to enrich understanding of these dynamics over time.

Implications: This research provides actionable insights for healthcare policymakers, digital health app developers, and hospital administrators by highlighting the importance of user trust and regulatory endorsement in enhancing mHealth app adoption. Strategic focus on data security and institutional backing can mitigate privacy concerns and foster user engagement in digital health platforms.

Keywords— Health Information Privacy Concerns, mHealth App Usage, Trust in mHealth App Security, Higher Authority Support

Introduction

1.1 Background

Mobile health (mHealth) apps have grown in numbers to allow users to avail health services, health monitoring, medical information, and connect with health care providers. Virtual hospital applications are becoming a more popular means of providing low-cost, convenient healthcare services, as reported by Wang et al. (2020). During the COVID-19 pandemic, the reliance on digital and remote healthcare services as substitutes for in-person care was further driven. Although these gains exist, privacy and security continue to be a challenge as mHealth applications gather and process personal and health sensitive data. Users' understanding and acceptance of digital health technologies might be affected by privacy concerns.

Liu and Tao (2022) have shown that lack of privacy has the potential to affect user trust and acceptance of smart healthcare services. Trust plays a significant role in mHealth adoption, as users who perceive mHealth services as trustworthy are more likely to intend to adopt them. Evidence also shows that privacy risk negatively influences both users' trust in mHealth services and their intention to adopt them (Deng et al., 2018). Thus, this study examines the influence of health information privacy, trust in app security, and higher-authority support on users' adoption of mHealth applications.

1.2 Problem Statement

Although mHealth applications are increasingly becoming available, privacy and

security concerns are still significant challenges to their adoption and use, especially for sensitive health information. Few studies have investigated the role of trust in app security in the relationships between health information privacy concerns and mHealth use, nor the impact of increased authority support on these relationships. Thus, the primary objective of this study is to examine how health information privacy concerns relate to the use of mHealth applications, while the trust in the security of the app acts as a mediator and higher authority support as a moderator.

1.3 Research Questions

The following are the research questions for the study:

1. Does health information privacy concerns has an impact on usage of mhealth apps?
2. Does health information privacy concerns as an impact on trust in mhealth app security?
3. Does trust in mhealth app security has an impact on usage of mhealth apps?
4. Does trust in mhealth app security mediates the relationship between health information privacy concerns and usage of mhealth apps?
5. Does higher authority support moderate the impact of trust in mhealth app security on usage of mhealth apps?

1.4 Significance of Study

mHealth applications have enhanced healthcare access, convenience, and patient engagement (Birkhoff & Smeltzer, 2021), although privacy and security issues are still significant obstacles to their broader use. The study explores the mechanisms by which health information privacy concerns affect the use of mHealth applications, including trust in the security of the app as a mediator and the level of support from higher authorities as a moderator. Privacy and security issues can result in users losing trust in mHealth applications and reducing their usage, as previous studies have shown that privacy concerns negatively impact trust in mobile health applications (Zhang et al., 2022).

Similarly, concerns regarding the privacy, security, and confidentiality of personal health information can negatively affect patients' adoption and use of mHealth applications, highlighting the importance of adequate privacy and security protections (Alhammad et al., 2024). The findings can help healthcare providers and mHealth developers strengthen privacy mechanisms, security measures, transparent privacy policies, and user trust. Implementing appropriate privacy and security safeguards can support the safe development and wider acceptance of mHealth applications in healthcare settings (Rezaee et al., 2023).

1.5 Research Objectives

The following is a list of the study's research objectives:

1. To examine the impact of health information privacy concerns on usage of mhealth apps.
2. To examine the impact of health information privacy concern on trust in mhealth app security.
3. To find out the impact of trust in mhealth app security on usage of mhealth apps.
4. To examine the mediating role of on trust in mhealth app security between health information privacy concern and usage of mhealth apps.

5. To explore the moderating role of higher authority support between trust in mhealth app security and usage of mhealth apps.

Literature Review

This chapter describes the relationships among the study variables and explains how health information privacy concerns, trust in mHealth app security, higher authority support, and usage of mHealth apps are related within the proposed research framework.

2.1 Overarching Theory PMT

According to Protection Motivation Theory (PMT), individuals' reactions to threats and their choices of protective responses involve threat appraisal and coping appraisal (Rogers, 1975). Threat appraisal is the extent to which users perceive a threat to their privacy, for example, through unauthorized access or data breaches, which could deter them from using mHealth apps, and coping appraisal is the extent to which users perceive the threat to their privacy is likely to be averted through the use of available security measures. Trust in security measures in mHealth app is proposed as a mediator as when users believe that the security mechanisms are effective and trustworthy, they are more willing to use mHealth applications. Healthcare institutions and regulators are suggested to act as a moderator to help build trust and drive adoption of mHealth apps. The use of Protection Motivation Theory (PMT) in technology privacy research has shown that individuals' perceptions of privacy threats can influence their concerns and decisions regarding the disclosure of personal information (Ioannou, 2021).

2.2 Health Information Privacy Concerns and Usage of mHealth

Health information privacy issues (HIPC) are user concerns about the collection, processing, storage, sharing and potential abuse or unauthorized disclosure of sensitive health information via mHealth applications. These concerns are especially relevant due to the need for the handling of personal health data in these services and the possibility of users not knowing how their data is being protected and utilized. Liu et al. (2022) concluded that privacy concerns play an important role in the adoption of mHealth services, and that the users' willingness to adopt mHealth services decreases when they are concerned about the leakage of health data and unauthorized use. However, privacy does not inevitably stop adoption from occurring; in cases where users believe they have adequate control over their information, transparency and protection, privacy perceptions are linked to acceptance. Similarly, Klaver et al. (2021) found that perceived privacy risk was related to reduced intention to use mHealth applications, which emphasizes the need for proper privacy protection to motivate people to adopt applications. Thus, promoting health information privacy concerns by providing transparency of data practices, user control and robust security measures is crucial to building confidence and engagement with mHealth applications, and the following hypothesis was proposed:

H1: Health information privacy concerns significantly and positively impact usage of mHealth apps.

2.3 Health Information Privacy Concerns and Trust in mHealth App Security

Trust in mHealth app security can be influenced by privacy issues, as people should

feel confident that their personal health data is being safeguarded and managed properly. The security of an mHealth app indicates the level of confidence users have in the app and its provider to handle health information responsibly and to prevent its unauthorized use or access. Studies have shown that trust in the provider, as well as perceived control over the personal data, are factors that affect the intent to use mHealth apps, and trust in the provider can be fostered to alleviate privacy concerns (Schomakers et al., 2022). Likewise, transparency of privacy policies and the power to control information can assist users in determining the level of protection an mHealth application offers. The importance of trust and perceived privacy in users' adoption of health-related mobile applications was also demonstrated by Fox et al. (2024), who found that users who experienced a sense of appropriate control and if data practices are not overly invasive, are more likely to have high levels of trust. Accordingly, increasing confidence in the security of mHealth applications by effective privacy protection, transparency, and user control can result in the following hypothesis:

H2: Health information privacy concerns significantly and positively impact Trust in mHealth app security.

2.4 Trust in mHealth App Security and Usage of mHealth Apps

Trust in mHealth app security is the trust users have in the security of the health app and mHealth providers, in the ability to keep their health information protected and to create a secure, dependable digital health space. In mHealth, trust is especially crucial as users are required to share personal and health data in order to receive digital health services. The findings of Binzer et al. (2024) indicate that there is a strong impact of trust in the health-app providers on intentions to use health applications, while the provider's governance affects how trust relates to perceived benefits, perceived risks, privacy control, and intentions to use health applications. Likewise, Klaver et al. (2021) revealed that trust had a positive association with the intention to use mHealth applications, indicating that if users view their information and interactions as sufficiently protected, they are more likely to engage with mHealth. Thus, trust can mitigate uncertainty, enhance confidence in the application, and promote ongoing interaction with mHealth services, which gives rise to the following hypothesis:

H3: Trust in mHealth app security significantly and positively impacts Usage of mHealth apps.

2.5 Mediating Role of Trust in mHealth App Security between Health Information Privacy Concerns and Usage of mHealth Apps

The use of mHealth could be affected by health information privacy concerns, as users consider how much their health information could be at risk due to its sharing, and then how well the app will keep it safe. Trust can thus serve as one of the psychological processes that transforms perceptions of privacy into intentions to act accordingly. Schomakers et al. (2022) showed that trust in the provider, the perceived control over personal data and privacy-related attitudes are important factors affecting mHealth usage intention, suggesting that trust is one of the key pathways between privacy perceptions and technology acceptance. Fox et al. (2024) also discovered that trust had a positive impact on adoption intent and the disclosure of information in health-related mobile apps and that perceived privacy also had an effect on adoption. The results

indicate that users might be more inclined to use the mHealth application if they feel secure about the application's security, data protection and control mechanisms, while still feeling concerned about privacy. Thus, trust in the security of mHealth apps could be an important factor that mediates the relationship between health information privacy concerns and mHealth use, which supports the following hypothesis:

H4: Trust in Mhealth app security mediates between Health information privacy concerns and usage of mHealth apps.

2.6 Moderating Role of Higher Authority Support between Trust in mHealth App Security and Usage of mHealth Apps

Higher authority support is endorsement, governance, guidance, and/or credibility provided by government agencies, health care institutions, regulatory authorities or other authorities that can impact the confidence of users in digital health applications. This could help reinforce the correlation between trust in app security and mHealth use by giving a further trust signal that an app is credible, properly governed, and has access to established privacy and security protocols. Binzer et al. (2024) identified that provider governance is an important factor in explaining the relationship between trust and health-app usage intentions, as users indicated a higher level of trust in health apps provided by a public provider compared to similar private providers. Likewise, Kang et al. (2024) illustrated that trust in government is a crucial part of the privacy calculus in the context of public-health mobile apps and found that trust in government can help shape users' perceptions and acceptance of health technologies. Thus, the level of the users' trust in the security of the mHealth application can potentially influence his/her level of usage, as may be predicted in the following hypothesis:

H5: Higher authority support moderates the relation between Trust in mHealth apps security and usage of mHealth apps in such a way that the relationship gets stronger when Higher authority support increases.

2.7 Research Model

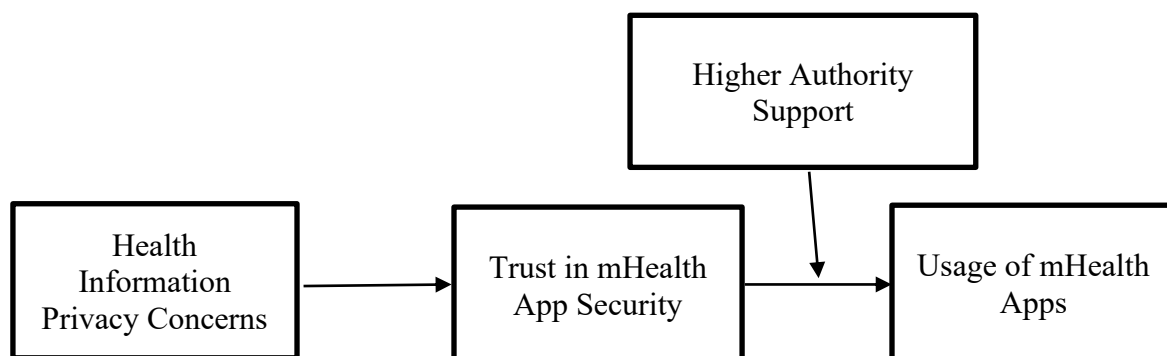


Figure 1. Proposed Research Model: Effect of Health Information Privacy Concerns on Usage of mHealth Apps, Having Trust in mHealth App Security as a Mediator and Higher Authority Support as a Moderator

Research Methodology

The research design, population, sample size, method of sampling, method of data collection and analysis method of data analysis in this study are explained in this chapter.

3.1 Research Design:

3.1.1 Type of Study:

The impact of health information privacy concerns on mHealth app usage is examined in this explanatory study, which also measures the moderating influence of higher authority support and trust in mHealth app security competency.

3.1.2 Study Setting:

Hospital employees and patients are the subjects of the study. In addition to filling out the surveys in their local institutions, participants from private hospitals in the twin cities of Rawalpindi and Islamabad will be contacted online via Google forms.

3.1.3 Time Horizon:

The data for this research is gathered throughout the study period and is cross-sectional in nature.

3.1.4 Research Interference:

This research is based on a field study and involves negligible research intervention. This study collects cross-sectional data. All variables' data are gathered by having participants complete a well-structured self-report questionnaire. Its cost-effectiveness also offers the benefit of minimizing researcher intervention, which lowers the potential for responder bias. This method makes it easier for respondents to complete the questionnaires and gives them the time they need to provide thoughtful, well-supported answers.

3.1.5 Unit of Analysis:

The unit of analysis for this research thesis are healthcare workers and patients of different private hospitals of twin cities.

3.2 Population and sampling:

3.2.1 Population:

Data from this study is collected from staff and patients of different private hospitals of twin cities i.e., Rawalpindi and Islamabad, Pakistan.

3.2.2 Sampling technique:

Convenience sampling, a non-probability sampling method, is used because it saves money and effort. This method works well and is easy to use. The personnel and patients of various private hospitals voluntarily participate in the data collection process, which is justified by the fact that gathering data from this demographic is simple and straightforward.

3.2.3 Sample size:

The rule of thumb of 10 items $\times$ 10 is used to calculate sample size. Because there are 22 items in total, the sample size in our case is 220 (22×10).

3.3 Scales and Measures

The measurement scales employed in this research include health information privacy concerns scale items, trust in mhealth app security scale items, usage of mhealth apps scale items, and higher authority support scale items and demographics.

3.3.1 Health Information Privacy Concerns

Health information privacy concerns are measured using (Wu et al. (2022) 3-item scale. One sample item for measuring this variable is ☐ I feel that it is not advisable to fill in personal health information in the online community. ☐ The Cronbach's alpha for this scale is 0.783.

3.3.2 Trust in mHealth App Security

Trust in mhealth app security is measured using a (Crane, 2018) 5-item scale. One sample item for measuring this variable is ☐ I am confident that Mhealth apps have strong security measures in place. ☐ The Cronbach's alpha for this scale is 0.633.

3.3.3 Higher Authority Support

Higher Authority Support is measured using a 6-item scale adapted from Sax and Torp (2015). One sample item for measuring this variable is ☐ Top management actively seeks middle managers' opinions and ideas on strategic issues. ☐ The Cronbach's alpha for this scale is 0.765.

3.3.4 Usage of mHealth Apps

Usage of mhealth app is measured using (Birkhoff, 2021) 8item scale. One sample item for measuring this variable is ☐ The amount of time involved in using this app has been fitting for me. ☐ The Cronbach's alpha for this scale is 0.963.

3.3.5 Control Variables:

One-way ANOVA and t-test are performed to control for variations in dependent variable(s), if any.

RESULTS

The major purpose of this study is to check out the impact of health information privacy on usage of mhealth apps with the mediating role of trust in mhealth app security and higher authority support as a moderator. This chapter presents the comprehensive results and analysis of the survey data, while the previous chapter describes the research methods used in this study. This chapter contains five sections that present quantitative analysis: demographic results, one-way ANOVA, descriptive analysis, regression/mediation, and moderation analysis of the variables used in the study. The dataset for the demographic variables is quantitatively analyzed in the first section. Subsequently, a thorough statistical analysis is conducted to evaluate every hypothesis formulated in this research model, which aims to investigate the relationship among health information privacy, usage of mhealth apps, trust in mhealth app security and higher authority support variables.

4.1 Quantitative Analysis

Quantitative analysis is used to provide context for the collected dataset. It aids in developing a deeper comprehension of the backgrounds and traits of the people. In addition to quantitative data (such as mean, standard deviation, etc.) of other variables like health information privacy, usage of mhealth apps, trust in mhealth app security and higher authority support, it includes the frequencies or distributions of demographic variables like gender, age, work status, education, and mhealth app usage frequency. The following subsections present quantitative data for each demographic variable in the form of tables.

4.1.1 Gender

Male and female possess distinct attitude and characteristics toward usage of mhealth apps which can cause a difference in the response. Out of 220 respondents, 49.2% are male and 50.8% are female.

4.1.2 Age

This research shows age demographics into four groups i.e. between 18 to 25, between 26 to 35, 36 to 50, and above 50. Out of 220 respondents, mostly individuals lie between the age group of 26 to 35.

4.1.3 Education

The 220 sample of the study displays that major respondents were having Graduation degrees i.e. 54%.

4.1.4 Mhealth App Usage Frequency

Out of 220 respondents, majority of respondents are from private settings, that is, 56.8%.

4.2 Control Variables

A one-way ANOVA was performed to control the variation in the usage of mHealth apps based on demographic variables used in the study. Results indicated a significant difference in usage of mHealth apps across age ($F=7.134$, $p < .05$), education ($F=4.646$, $p < .05$), mHealth App usage frequency ($F=0.282$, $p < .05$), while no significant difference was found in gender. (Table 1).

Table 1. One Way ANOVA

Demographics	UMA	
	f value	p value
Gender	12.937	0.000
Age	7.134	0.000
Education	4.646	0.004
mHealth App usage frequency	0.282	0.754

N= 220, Abbreviations: UMA, Usage of mHealth Apps

4.3 Descriptive Analysis

Descriptive statistics are used to examine the data as a table and determine the mean and standard deviation of each variable. The results are shown below in table 2. Skewness and Kurtosis in table 3 shows that data is normally distributed as their values lie between the normal range i.e. skewness +2 to -2 and kurtosis +7 to -7. Hair et al. (2010) and Bryne (2010) supported similar results.

Table 2. Descriptive statistics

	Mean	Standard deviation
HIPC	4.05	.82
TMAS	4.07	.72
HAS	4.04	.74
UMA	3.00	.81

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

N= 220, Abbreviations: HIPC, Higher Information Privacy Concerns; TMAS, Trust in mHealth App Security; HAS, Higher Authority Support; UMA, Usage of mHealth Apps.

Table 3. Skewness & Kurtosis

	Skewness	Kurtosis
HIPC	-1.637	3.060
TMAS	-1.911	4.908
HAS	-1.617	3.786
UMA	0.470	-0.036

N= 220, Abbreviations: HIPC, Higher Information Privacy Concerns; TMAS, Trust in mHealth App Security; HAS, Higher Authority Support; UMA, Usage of mHealth Apps.

4.4 Correlations

Correlation analysis displays the connection among the variables. It explains how strong or weak association lies among the variables. The correlation coefficient of the variables is reported in Table 4.

Table 4. Correlation Analysis

	1	2	3	4
1. Health Information Privacy Concerns	1			
2. Trust In mHealth App Security	.154*	1		
3. Higher Authority Support	.315*	.202*	1	
4. Usage of mHealth Apps	.242*	.239*	.257*	1

N=220, *p<.05

The table shows the correlation effect of each variable on the other. All these variables are highly correlated with each other. Health information privacy concerns is positively correlated with their trust in mhealth app security ($r=0.154$, $p<0.01$), higher authority support ($r=0.315$, $p<0.01$) and usage of mhealth apps ($r=0.242$, $p<0.01$). Trust in mhealth security has significant and positive correlation with higher authority support ($r=0.202$, $p<0.01$) and usage of mhealth apps ($r=0.239$, $p<0.01$). Higher authority support is positively correlated with usage of mhealth apps ($r=0.257$, $p<0.01$).

4.5 Regression Analysis

The results in table 5, indicate that health information privacy concerns have a significant and positive effect on trust in mHealth app security, with a standardized coefficient ($B = 0.754$, $p < .001$). Moreover, health information privacy concerns significantly influence usage of mHealth apps ($B = 0.242$, $p < .001$). Finally, trust in

mHealth app security has a strong positive impact on usage of mHealth apps ($B = 0.239$, $p < .001$). These results confirm the direct effects among the key constructs and show that hypotheses H1, H2, and H3 are supported.

Table 5. Regression Analysis (Direct Effects)

Hypothesis	Relationship	B	SE	T	P
H1	HIPC→UMA	0.242	0.041	5.90	0.000
H2	HIPC→TMAS	0.754	0.034	22.18	0.000
H3	TMAS→UMA	0.239	0.049	4.88	0.000

N= 220, Abbreviations: HIPC, Health Information Privacy Concerns; TMAS, Trust in mHealth App Security; UMA, Usage of mHealth Apps

4.6 Regression/Mediation Analysis

The mediation results in table 6, show that trust in mHealth app security mediates the relationship between health information privacy concerns and usage of mHealth apps. When trust in mHealth app security is included in the model, the direct effect of health information privacy concerns on usage of mHealth apps becomes statistically non-significant ($B = 0.073$, $p = 0.111$). However, the indirect effect through trust is statistically significant ($B = 0.180$, 95% CI: 0.117 to 0.263). These results confirm full mediation, thereby supporting hypothesis H4.

Table 6. Regression/Mediation Analysis

Path	B	SE	T	P
HIPC→TMAS	0.754	0.034	22.18	0.000
TMAS→UMA	0.239	0.049	4.88	0.000
HIPC→UMA (Direct effect controlling for TMAS)	0.073	0.045	1.60	0.111
Bootstrap results for indirect effect	Indirect effect	LL 95% CI	UL 95% CI	
	0.180	0.117	0.263	

N= 220, Abbreviations: HIPC, Higher Information Privacy Concerns; TMAS, Trust in mHealth App Security; UMA, Usage of mHealth Apps.

4.7 Moderation Analysis

The moderation results in Table 7 demonstrate that higher authority support moderates the relationship between trust in mHealth app security and usage of mHealth apps. The interaction effect of TMAS × HAS is significant ($B = 0.071$, $p = 0.026$), indicating that when higher authority support is high, the positive effect of trust in mHealth app security on usage of mHealth apps becomes stronger. Hence, hypothesis H5 is supported.

Table 7. Moderation Results (Bootstrapping)

Predictor	PS			
	B	R ²	ΔR ²	p-Values
Step 1		0.043		

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Control Variables	—	—	—	—
Step 2	—	0.231	0.188	0.000
TMAS	0.211	—	—	0.000
HAS	0.166	—	—	0.001
Step 3		0.273	0.042	0.026
TMAS×HAS (Interaction Term)	0.071	—	—	0.026

N= 220, Abbreviations: HAS, Higher Authority Support; TMAS, Trust in mHealth App Security.

DISCUSSION

Chapter 4 presents the findings and data analysis of the study. This chapter explains the relationships among the study variables and examines the proposed hypotheses regarding the effect of health information privacy concerns on mHealth app usage. Trust in mHealth app security is examined as a mediator, while higher authority support is examined as a moderator. The results of the statistical analyses are presented and interpreted for each hypothesis, with detailed findings provided below.

5.1 Health Information Privacy Concerns and Usage Of mHealth Apps

The first hypothesis of the present research study was: Health information privacy concerns significantly and positively impact usage of mHealth apps. Results from the regression analysis indicated that there was a significant and positive relationship between health information privacy concerns and mHealth app usage, thus supporting H1. This is similar to the results of Fox et al., (2024), which revealed that trust and perceived privacy positively affected users' intention to use health-related mobile applications and willingness to disclose personal information. Likewise, Schomakers et al. (2022-) found that trust in the mHealth provider was a key factor in users' intention to use mHealth applications and that perceived control over their personal information led to users' trust. Moreover, Taneski et al. (2026) found that privacy policies in mHealth applications were often lengthy, difficult to understand, and vague about how users' health data were collected and processed, highlighting the importance of clear and transparent privacy practices in building users' confidence and supporting the use of mHealth applications. Shojaei et al. (2025) also reported that users noted that transparency, control over the personal data, clear privacy policies, and security measures were key factors in developing trust and acceptance of mHealth applications. This is in line with Protection Motivation Theory (PMT) which states that the user may practice protection behaviour when they are aware of a threat, but also think that they can do something about it to minimize the risk of the threat. While privacy concerns might lead to reluctance to use mHealth, users may be more inclined to use apps that offer transparency regarding privacy, robust security features, and increased control over their health information.

5.2 Health Information Privacy Concerns and Trust in mHealth App Security

The second hypothesis of the present study was: *Health information privacy concerns significantly and positively impact Trust in mHealth app security.* The regression

analysis supported H2 that said there was a significant and positive relationship between health information privacy concerns and trust in mHealth app security. Liu and Tao (2022) identified loss of privacy as an important antecedent of smart healthcare services acceptance, and trust as a mediator between loss of privacy concerns and users' acceptance. Similarly, Zhang et al. (2022) found that privacy and security concerns were significant factors to consider for the adoption of mHealth services, and security features like consent, access and personal health information protection were valued by users. Additionally, Gupta et al. (2023) showed that certain privacy measures, such as data transparency, oversight, and data deletion measures, were linked to higher levels of willingness to share personal digital health information, indicating that visible protections can increase user's trust in digital health services.

Furthermore, Iwaya et al. (2023) noted that privacy concerns and safeguarding sensitive data continue to be significant issues in mental health apps, and they called for more robust privacy measures in mHealth technologies. The results are also consistent with Protection Motivation Theory (PMT) which suggests that users who feel a threat to their privacy will consider how well the measures available can protect them before they choose to use a DH service. Therefore, better transparency in privacy practices, robust security measures, and the ability for users to have more control over their personal health information can help mitigate the perceived privacy threats and enhance trust in mHealth applications.

5.3 Trust in mHealth App Security and Usage of mHealth App

The third hypothesis of the current research study was: *Trust in mHealth app security significantly and positively impacts Usage of mHealth apps*. The regression analysis showed a positive relationship between trust in the security of mHealth apps and mHealth app use, indicating that H3 was supported. The sensitive health data collected and processed by mHealth applications can impact privacy and security concerns, which can influence users' willingness to adopt and continue using the application. He (2023), in his study of 625 users of mobile medical platforms in China, discovered that trust positively affected users' intentions to use mobile medical platforms and technical risk concerns negatively moderated the relationship between trust and use intention.

The study specifically found that privacy and security issues were important dimensions of technical risk, meaning that users who felt that there was more risk from the technological side may be less inclined to turn their trust into real intentions for using the product. Likewise, Tamime et al. (2024) studied privacy issues with health applications using 432 scenarios of health data exchange evaluated by 189 individuals. Their results indicated that users had concerns about privacy, especially concerning sharing of data, in all types of health-data exchanges. The results suggest that the worries about the collection, sharing, and safeguarding of personal health information might affect how consumers view mHealth applications and their readiness to utilize these technologies. In terms of Protection Motivation Theory (PMT), such concerns can be seen as perceptions of potential threats which could affect an individual's protective evaluations and their technology decisions. Thus, if individuals think that there is a higher risk of their health information being compromised, they are less likely to use

mHealth apps, and higher confidence in these platform's security is more likely to promote use of mHealth apps.

5.4 Mediating Role of Trust in mHealth App Security between Health information privacy concerns and usage of mHealth apps

The fourth hypothesis of the current research study was: *Trust in mHealth app security mediates between Health information privacy concerns and usage of mHealth apps.* The mediation analysis results revealed that the indirect path of health information privacy concerns on the use of mHealth apps via trust in health security apps was significant, this supported H4. The result suggests that privacy concerns affect usage in part because of the trust that is gained by users regarding the security and data protection of an app. Sun et al. (2022) reported that trust in the platforms has a positive impact on users' willingness to share their personal information, and that privacy concerns have a negative impact on their satisfaction with the online healthcare platform. Their results indicate that the trust and privacy of the users is a key factor in their willingness to provide personal information when utilizing digital healthcare services.

Binzer et al. (2024) reported that trust in health-app providers was associated with users' intentions to use health applications. Their findings further showed that perceived privacy control and perceived risks are important factors through which trust relates to usage intentions, highlighting the importance of trustworthy and privacy-conscious mHealth services. Fu et al. (2024) found that privacy concerns were negatively associated with user engagement in mHealth applications, while perceived privacy partially mediated this relationship. The study further showed that greater perceived control over personal data reduced the negative effect of privacy concerns on engagement, suggesting that effective privacy management can support sustained mHealth app use. These results align with PMT as privacy concerns are first identified and then assessed if security measures are able to safeguard the user; once trust in the security measures is developed, privacy concerns are more likely to become continued usage. This implies that trust in the security of mHealth apps is a crucial psychological link between privacy concerns and use of mHealth.

5.5 Moderating Role of Higher Authority Support Between Trust in mHealth App Security and Usage of mHealth App

The fifth hypothesis of the present research study was: *Higher authority support moderates the relation between Trust in mHealth apps security and usage of mHealth apps in such a way that the relationship gets stronger when Higher authority support increases.* The fifth hypothesis of the present research study was: The relation between Trust in mHealth apps security and mHealth apps use will be strengthened with the increase of the Higher authority support. The results from the moderation analysis indicated that there was no significant interaction between trust in mHealth app security and higher authority support, so that H5 was not supported. This discovery implies that credentialing (institutional or leadership) might be useful to add credibility, but it is not likely to greatly amplify individual trust's influence on mHealth. Likewise, external and institutional support can have different impacts on mHealth use depending on users' trust, perceived risks, and privacy control, as revealed from earlier studies. Binzer et al.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

(2024) found that provider governance had a significant impact on the content of the trust-health app usage intentions relationship, especially relating to perceived risks and privacy control. They also found that there was a correlation between public health-app providers and trust, and that to a certain degree, governance and regulation could replace trust in users' perceptions of privacy and security.

Furthermore, Zhu et al. (2021) illustrated that privacy concerns are not necessarily reflected in privacy-related behaviors, which underscored the need for users' privacy evaluations and perceptions of app information-management practices. Further, studies on wearable health technologies suggests that trust is a mediator between perceived privacy and security, and intention to use the technology (Adebessin & Mwalugha, 2020). While higher authority support could enhance users' beliefs in the security and legitimacy of mHealth apps, it could rely on how much users trust the app, feel secure with it, and believe it can keep their health information safe.

5.6 Practical Implications

The results have implications for mHealth developers, healthcare practitioners, policymakers, healthcare institutions, and educators. Given the importance of privacy, trust in mHealth app security and authority support to mHealth usage, stakeholders should engage in a coordinated effort to enhance privacy, security and user confidence in the use of mHealth. Healthcare institutions should make use of mHealth apps that adhere to well-known data-protection guidelines like HIPAA and GDPR, and conduct frequent security audits, encryption, authentication, and risk evaluations. Both developers and users should embrace principles of privacy by design and user-centricity, including robust security measures, user-friendly data sharing transparency, and user-friendly explanations of security measures. Healthcare leaders and public health authorities, via endorsement systems, certification or approved-app registries, and educators, should foster secure and credible apps by educating healthcare students on digital literacy, ethics in health-data usage, privacy, and cybersecurity.

Awareness programs at the patient level should enable users to comprehend and understand privacy policies, to control app permissions, to be aware of security threats, and to report violations, especially digitally underserved groups. By bringing together the healthcare institutions, developers, regulators, and professional bodies, the combination of institutional credibility and technological reliability can be achieved. In Pakistan, there is a need for localized mHealth guidelines for privacy and security, with easy access to complaints, notification of data breaches, and penalties for non-compliance. Overall, future mHealth projects should focus on privacy by design, trust-building security measures, institutional partnerships and ongoing training to enable secure and sustainable mHealth use.

5.7 Limitations, Future Directions, and Recommendations

The need for recognition and declaration of any possible constraints is important for any research which is carried out. When researching a topic, researchers encounter a number of difficulties. The problems faced are instrumental problems, problems in data collection, restrictions and financial constraints, and having a larger population. These are some of the problems and contestations that limit any research project. These problems are a stimulus to other researchers to revisit the topic with more successful

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

methods and environments. The research study is bounded and recommendations are given below.

5.7.1 Limitations

There are a number of limitations in this study that should be taken into account when interpreting the findings and which their conclusions might have relied on. The findings obtained from the non-probability convenience sampling method may be limited to the generalizability and representativeness of 220 health care practitioners from facilities in Islamabad and Rawalpindi in Pakistan. Additionally, the cross-sectional design and online questionnaire limit the ability to draw causal inferences and can also cause voluntary response and common method biases. The study was based solely on quantitative self-reported data from healthcare professionals, which might have affected the results and findings due to the individual experiences and perceptions of the respondents, and the lack of qualitative responses prevented deeper insights into the issues of privacy, trust and mHealth use. Furthermore, the participants were in various professional designations and institutions which had not been completely standardized, and other relevant groups, e.g., patients, healthcare users outside of a professional setting, were not included.

5.7.2 Future Directions and Recommendations

Future studies should address these limitations by incorporating more time to study changes and causal relationships over time (longitudinal design), and better representativeness through probability or random sampling. Larger and more diverse samples across various regions of Pakistan and a wider range of healthcare professionals and patients and other mHealth users should be encouraged to take part in studies. The analysis of the experiences with, and concerns about privacy, trust and security perceptions of users should also include mixed methods or qualitative methods for a deeper understanding. Other individual and organizational factors, including digital literacy, perceived usefulness, data sensitivity, IT support, app usability, user satisfaction, perceived behavioral control, institutional culture, and regulatory environment, and other mediators and moderators could be explored by future researchers. Measured scales might also be evaluated in other settings and groups. Face-to-face data collection and open-ended questions might decrease limitations on responses and yield more information. Finally, the research should be expanded to include all provinces and various regions of Pakistan to have more evidence of mHealth adoption and for the better generalizability of the findings for the country.

Conclusion

Regardless of the growing interest in digital health technologies, there is still a need for systematic research focusing on psychological and institutional factors that influence the adoption of mHealth applications, especially in developing healthcare systems. Therefore, our research contributes to the existing body of knowledge by offering evidence that trust in mHealth app security significantly mediates the relationship between health information privacy concerns and mHealth app usage. The levels of health information privacy concerns, trust in app security, and the moderating role of higher authority support have all been assessed in this study to understand their

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

combined influence on the behavioral intention to use mHealth apps.

Our analysis confirmed significant support for most of the hypotheses in the model, with trust in app security playing a pivotal mediating role. However, the moderation analysis showed that higher authority support does not significantly strengthen the relationship between trust and usage, which may be attributed to contextual factors such as cultural influences, institutional limitations, or personal autonomy in health technology usage. Several explanations may exist for why healthcare professionals rely more on personal judgment and less on organizational encouragement when it comes to using mobile health apps. Including previous experiences with the digital platforms, perceived self-efficacy in managing technology, and the perceived credibility of the institution promoting the app.

Employees working in hospitals especially those at the frontline of patient care, should have strong digital literacy and an understanding of data privacy principles to ensure effective, ethical, and secure delivery of mobile health services. The presence of health information privacy concerns is a critical factor and is unignorable. This has a direct impact on the confidence and trust required for active engagement with mHealth tools. Our findings demonstrate that addressing these privacy concerns through visible security measures and institutional transparency leads to greater trust, which in turn boosts app adoption.

In training programs there should be a focus on the understanding of mobile health app functionality and digital ethics must be enhanced. Our study also emphasizes the need to promote trust through both technology design and institutional behavior, including consistent communication, visible support from health authorities, and ethical data governance practices. When these mechanisms are not present, even a trusted platform may not reach its full potential due to lack of confidence of end user.

References

- Adebesin, F., & Mwalugha, R. (2020). The mediating role of organizational reputation and trust in the intention to use wearable health devices: Cross-country study. *JMIR mHealth and uHealth*, 8(6), e16721.
- Alhammad, N., Alajlani, M., Abd-alrazaq, A., Epiphaniou, G., & Arvanitis, T. (2024). Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: Systematic review. *Journal of Medical Internet Research*, 26, e50715.
- Birkhoff, S. D. (2021). Facilitators and challenges in the adoption of a virtual nurse visit in the home health setting. *Home Health Care Services Quarterly*, 40(2), 105–120.
- Binzer, B., Kendziorra, J., Witte, A.-K., & Winkler, T. J. (2024). Trust in public and private providers of health apps and usage intentions: A sectoral privacy calculus and control perspective. *Business & Information Systems Engineering*, 66(3), 273–297.
- Deng, Z., Hong, Z., Ren, C., Zhang, W., & Xiang, F. (2018). What predicts patients' adoption intention toward mHealth services in China: Empirical study. *JMIR mHealth and uHealth*, 6(8), e172.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- Fox, G., van der Werff, L., Rosati, P., & Lynn, T. (2024). Investigating citizens' acceptance of contact tracing apps: Quantitative study of the role of trust and privacy. *JMIR mHealth and uHealth*, 12, e48700.
- Fu, S., Chen, X., Liang, S., et al. (2024). Understanding user engagement in mobile health applications from a privacy management perspective. *Health Promotion International*, 39(4), daae103.
- Gupta, R., Iyengar, R., Sharma, M., et al. (2023). Consumer views on privacy protections and sharing of personal digital health information. *JAMA Network Open*, 6(3), e231305.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Pearson.
- He, J. (2023). The impact of users' trust on intention to use the mobile medical platform: Evidence from China. *Frontiers in Public Health*, 11, 1076367.
- Iwaya, L. H., Babar, M. A., Rashid, A., & Wijayarathna, C. (2023). On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering*, 28(1), Article 2.
- Kang, H., Lee, J. K., Lee, E. W. J., & Toh, C. (2024). The roles of trust in government and sense of community in the COVID-19 contact tracing privacy calculus: Mixed method study using a 2-wave survey and in-depth interviews. *JMIR mHealth and uHealth*, 12, e48986.
- Klaver, N. S., van de Klundert, J., van den Broek, R. J. G. M., & Askari, M. (2021). Relationship between perceived risks of using mHealth applications and the intention to use them among older adults in the Netherlands: Cross-sectional study. *JMIR mHealth and uHealth*, 9(8), e26768.
- Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior*, 127, 107026.
- Ioannou, A. (2021). Dispositional mindfulness as an antecedent of privacy concerns: A protection motivation theory perspective. *Psychology & Marketing*, 38(12), 2219–2232.
- Rezaee, R., Khashayar, M., Saeedinezhad, S., Nasiri, M., & Zare, S. (2023). Critical criteria and countermeasures for mobile health developers to ensure mobile health privacy and security: Mixed methods study. *JMIR mHealth and uHealth*, 11, e39055.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.
- Sax, J., & Torp, S. S. (2015). Speak up! Enhancing risk performance with enterprise risk management, leadership style and employee voice. *Management Decision*, 53(7), 1452–1468.
- Schomakers, E.-M., Lidynia, C., Vervier, L. S., Calero Valdez, A., & Ziefle, M. (2022). Applying an extended UTAUT2 model to explain user acceptance of lifestyle and therapy mobile health apps: Survey study. *JMIR mHealth and uHealth*, 10(1), e27095.
- Sun, S., Zhang, J., Zhu, Y., Jiang, M., & Chen, S. (2022). Exploring users' willingness

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- to disclose personal information in online healthcare communities: The role of satisfaction. *Technological Forecasting and Social Change*, 178, 121595.
- Shojaei, P., Chow, Y.-W., & Vlahu-Gjorgievska, E. (2025). User privacy concerns and preferences in mHealth applications: Balancing privacy and usability. *Studies in Health Technology and Informatics*, 329, 229–233.
- Taneski, V., Schwarz, P., Bošnjak, L., Tropmann-Frick, M., & Brumen, B. (2026). Readability and vagueness of privacy policies in mHealth applications: A multi-country analysis. *International Journal of Information Security*, 25, Article 35.
- Tamime, R. A., Farooq, A., Salminen, J., Marmion, V., & Hall, W. (2024). Understanding privacy concerns in mobile health applications: A scenario-based online survey. In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1757–1765). IEEE.
- Wang, Y., Liu, Y., Shi, Y., Yu, Y., & Yang, J. (2020). User perceptions of virtual hospital apps in China: Systematic search. *JMIR mHealth and uHealth*, 8(8), e19487.
- Wu, B., Luo, P., Li, M., & Hu, X. (2022). The impact of health information privacy concerns on engagement and payment behaviors in online health communities. *Frontiers in Psychology*, 13, 861903.
- Zhang, J., Luximon, Y., & Li, Q. (2022). Seeking medical advice in mobile applications: How social cue design and privacy concerns influence trust and behavioral intention in impersonal patient–physician interactions. *Computers in Human Behavior*, 130, 107178.
- Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, 61, 101601.

Appendix:

Scale: Responses to each item are measured on a five-point scale with the options:

(1) strongly disagree, (2) disagree, (3) neither disagree nor agree, (4) agree, (5) strongly agree.

An (R) denotes a negatively phrased and reverse-scored item.

SECTION A

HEALTH INFORMATION PRIVACY CONCERNS

I feel that it is not advisable to fill in personal health information in the online community.	1	2	3	4	5
Once the personal health information in the online health community is filled in, it will be abused by companies.	1	2	3	4	5
Once the personal health information in the online health community is filled in, it will be shared by the company or sold to	1	2	3	4	5

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

	others.					
--	---------	--	--	--	--	--

Health Information Privacy Concerns were measured using items adapted from Wu et al. (2022).

SECTION B

TRUST IN MHEALTH APP SECURITY

1	I trust that my personal health data is secure when using Mhealth App.	1	2	3	4	5
2	I believe that Mhealth apps protect my data from unauthorized access.	1	2	3	4	5
3	I am confident that Mhealth apps have strong security measures in place.	1	2	3	4	5
4	I trust that Mhealth apps do not share my data with third parties without my consent.	1	2	3	4	5
5	I feel safe using Mhealth apps to manage my health-related information.	1	2	3	4	5

Crane (2018). mHealth Apps usage in patients. *On-Line Journal of mHealth Apps usage*, 13(4).

SECTION C

HIGHER AUTHORITY SUPPORT

1	Top management actively seeks middle managers' opinions and ideas on strategic issues.	1	2	3	4	5
2	Top management is open to new ideas and initiatives from ERM team member.	1	2	3	4	5
3	Top management appreciate that middle manager's experiments with new ideas and products.	1	2	3	4	5
4	Top management appreciate that middle manager's experiments on new products.	1	2	3	4	5
5	Top management ensures that the interest of middle managers is considered when making strategic decisions.	1	2	3	4	5
6	The organization establish a risk management committee at various level to measure the commitment of top management.	1	2	3	4	5

Higher Authority Support is measured using a 6-item scale adapted from Sax and Torp (2015).

SECTION D

USAGE OF MHEALTH APPS

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

1	The app was easy to use.	1	2	3	4	5
2	It was easy for me to learn to use the app.	1	2	3	4	5
3	I like the interface of the app.	1	2	3	4	5
4	The information in the app was well organized, so I could find the information I needed.	1	2	3	4	5
5	I feel comfortable using this app is social settings.	1	2	3	4	5
6	The amount of time involved in using this app has been fitting for me.	1	2	3	4	5
7	I would use this app again.	1	2	3	4	5
8	Overall, I am satisfied with this app.	1	2	3	4	5

Birkhoff (2021). Telehealth Apps in patients. *On-Line Journal of Telehealth usage*, 33(7).

DEMOGRAPHIC QUESTIONS

Please Circle the Appropriate Answer.

- 1. Gender:** **A. Male** **B. Female**
- 2. Education:** **A. Single** **B. Married**
- 3. Age:** **A. 18-25** **B. 26-35** **C. 36-50** **D. Over 50**
- 4. Mhealth App Usage Frequency:** **A. Daily** **B. Weekly** **C. Monthly** **D. Rarely**