Patients and Stakeholders' Perspectives Regarding the Privacy, Security, and Confidentiality of Data Collected via mHealth Apps in Saudi Arabia: A Protocol for a Mixed Method Study

Nasser Alhammad, Mohannad Alajlani, Alaa Abd-alrazaq, Theodoros Arvanitis, Gregory Epiphaniou

Submitted to: JMIR Research Protocols
on: November 28, 2023

Table of Contents

Patients and Stakeholders' Perspectives Regarding the Privacy, Security, and Confidentiality of Data Collected via mHealth Apps in Saudi Arabia: A Protocol for a Mixed Method Study

Nasser Alhammad[1, 2] MSc; Mohannad Alajlani[1] PhD; Alaa Abd-alrazaq[3] PhD; Theodoros Arvanitis[4] PhD; Gregory Epiphaniou[1] PhD

[1]University of Warwick Coventry GB
[2]Saudi Electronic University Jeddah SA
[3]AI Center for Precision Health, Weill Cornell Medicine Doha QA
[4]University of Birmingham Birmingham GB

Corresponding Author:
Nasser Alhammad MSc
University of Warwick
Institute of Digital Healthcare, WMG
Coventry
GB

Abstract

Background: There is data paucity regarding users' awareness of privacy concerns and the resulting impact on the acceptance of mHealth apps, especially in the Saudi context. Such information is pertinent in addressing users' needs in the Kingdom of Saudi Arabia (KSA).

Objective: This article presents a study protocol for a mixed-method analysis to assess the patients' and stakeholders' perspectives regarding the privacy, security, and confidentiality of data collected via mHealth apps in the KSA and the factors affecting the adoption of mHealth apps.

Methods: An exploratory mixed-method study design methods will be employed. Patients and end-users of mHealth apps will be randomly recruited from 4 purposively selected hospitals in Saudi Arabia for the quantitative phase (i.e., survey). The research instrument will be developed based on the emerging themes and findings from the interview conducted among stakeholders, app developers, healthcare professionals and users of mHealth apps (n = 25). The survey will focus on 1) how to improve patients' awareness of data security, privacy, and confidentiality, (2) feedback on the current mHealth apps in terms of data security, privacy, and confidentiality, (3) the features that might improve data security, privacy, and confidentiality of mHealth apps. Meanwhile, specific sections of the questionnaire will focus on patients' awareness, privacy concerns, confidentiality concerns, security concerns, perceived usefulness, perceived ease of use, and behavioural intention. Qualitative data will be analysed thematically using NVIVO version 12. Descriptive statistics, regression analysis, and structural equation modelling will be performed using SPSS and PLS-SEM.

Results: The ethical approval for this research has been obtained from the Biomedical and Scientific Research Ethics Committee, University of Warwick (REF:) and the Medical Research & Ethics Committee Ministry of Health in the KSA. The qualitative phase is ongoing and 15 participants have been interviewed. The interviews for the remaining 10 participants will be completed by 25 November 2023. Preliminary thematic analysis is still ongoing. Meanwhile, the quantitative phase will commence by December 10, 2023, with 150 participants providing signed and informed consent to participate in the study.

Conclusions: The mixed methods study will elucidate the antecedents of patients' awareness and concerns regarding the privacy, security, and confidentiality of data collected via mHealth apps in Saudi Arabia. Furthermore, pertinent findings on the perspectives of stakeholders and healthcare professionals toward the aforementioned issues will be gleaned. The results will assist policymakers in developing strategies to improve Saudi users'/patients' adoption of mhealth apps and addressing the concerns raised in order to benefit significantly from these advanced healthcare modalities.

(JMIR Preprints 28/11/2023:54933)
DOI: https://doi.org/10.2196/preprints.54933

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

Please make my preprint PDF available to anyone at any time (recommended).

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.

Only make the preprint title and abstract visible.

✓ **No, I do not wish to publish my submitted manuscript as a preprint.**

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Original Paper

N. Alhammad[1], M. Alajlani[1], A. Abd-alrazaq[2], T.N. Arvanitis[3] and G. Epiphaniou[1]

[1]Institute of Digital Healthcare, WMG, University of Warwick, Coventry, CV4 7AL, United Kingdom

[2]AI Center for Precision Health, Weill Cornell Medicine, Doha, Qatar
[3]School of Engineering, University of Birmingham, Edgbaston, Birmingham, B15 2TT, United Kingdom

Patients and Stakeholders' Perspectives Regarding the Privacy, Security, and Confidentiality of Data Collected via mHealth Apps in Saudi Arabia: A Protocol for a Mixed Method Study

Abstract

Background: There is data paucity regarding users' awareness of privacy concerns and the resulting impact on the acceptance of mHealth apps, especially in the Saudi context. Such information is pertinent in addressing users' needs in the Kingdom of Saudi Arabia (KSA).

Objectives: This article presents a study protocol for a mixed-method analysis to assess the patients' and stakeholders' perspectives regarding the privacy, security, and confidentiality of data collected via mHealth apps in the KSA and the factors affecting the adoption of mHealth apps.

Methods: A mixed-method study design methods will be employed. In the quantitative phase, patients and end-users of mHealth apps will be randomly recruited from the various pronvinces in Saudi Arabia with high population of mHealth users. The research instrument will be developed based on the emerging themes and findings from the interview conducted among stakeholders, app developers, healthcare professionals and users of mHealth apps (n = 25). The survey will focus on 1) how to improve patients' awareness of data security, privacy, and confidentiality, (2) feedback on the current mHealth apps in terms of data security, privacy, and confidentiality, (3) the features that might improve data security, privacy, and confidentiality of mHealth apps. Meanwhile, specific sections of the questionnaire will focus on patients' awareness, privacy concerns, confidentiality concerns, security concerns, perceived usefulness, perceived ease of use, and behavioural intention. Qualitative data will be analysed thematically using NVIVO version 12. Descriptive statistics, regression analysis, and structural equation modelling will be performed using SPSS and PLS-SEM.

Results: The ethical approval for this research has been obtained from the Biomedical and Scientific Research Ethics Committee, University of Warwick and the Medical Research & Ethics Committee Ministry of Health in the KSA. The qualitative phase is ongoing and 15 participants have been interviewed. The interviews for the remaining 10 participants will be completed by 25 November 2023. Preliminary thematic analysis is still ongoing. Meanwhile, the quantitative phase will commence by December 10, 2023, with 150 participants providing signed and informed consent to participate in the study.

Conclusions: The mixed methods study will elucidate the antecedents of patients' awareness and concerns regarding the privacy, security, and confidentiality of data collected via mHealth apps in Saudi Arabia. Furthermore, pertinent findings on the perspectives of stakeholders and healthcare professionals toward the aforementioned issues will be gleaned. The results will assist policymakers in developing strategies to improve Saudi users'/patients' adoption of mhealth apps and addressing

the concerns raised in order to benefit significantly from these advanced healthcare modalities.

KEYWORDS: Awareness, data privacy, confidentiality, security, healthcare, patients, Saudi Arabia, mHealth, mobile apps

Introduction

Background

In recent years, the usage of mHealth apps by both public and healthcare professionals (HCPs) significantly increased with the introduction of smartphones [1] and growing interest in the healthcare industry and research field [2]. The coronavirus disease 2019 pandemic has further accelerated reliance on digital health [3]. mHealth apps are used to manage diseases, self-monitoring, gather health information, supervise behavioural changes, manage fitness, and remind patients of their medication and rehabilitation schedules [4]). From the HCPs' view, mHealth apps help manage health records, provide easy access to health records, and provide a path to conduct mobile consultation and remote monitoring during and after treatment [5]).

Healthcare professionals like physicians are the second-largest stakeholders within the healthcare field after patients. Thus, mhealth apps connected to clinical information systems (CICs) permit healthcare professionals to access patients' databases [6] . One of the prime goals urging the adoption of mhealth apps among healthcare professionals is providing timely consultation and decision-making at the point of care, which require different resources, especially clinical data from CISs. CISs are part of the hospital information systems (HISs), directly linked to inpatient and outpatient care. The main advantage of these systems is that they can be connected to other subsystems within a hospital, like different departments and laboratories [7] . Clinicians rely on this system when making decisions on their patients' health. Therefore, patients are compelled to use CISs, especially when the healthcare provider offers care only through the mhealth apps. Although connecting CISs with mhealth apps simplifies hospital workflows but still creates new challenges, such as data confidentiality and security. Data confidentiality, privacy, security, and regulatory supervision of the apps are known barriers that hinder mHealth adoption in the HC field [8].

Confidentiality refers to the responsibility of those who obtain data/information (app providers) to uphold the solitude concerns of those to whom the information is related (consumers) [8]. Meanwhile, according to the National Committee on Vital and Health Statistics (NCVHS), privacy refers to an individual legal right or freedom to protect or disclose their health information, and security is explained as personal, mechanical, or authority protection tools used to guard the health information against unwanted people or access. Security, on the other hand, is defined as the physical, mechanical, or legislative mechanism or tools to shield personal health information from unauthorised disclosure [8]. There are several reasons for data protection in mhealth applications, such as keyed-in information being susceptible and mobile apps being of interest to attackers or hackers [7]. In addition, data management and storage, data privacy disclosure, data integration, data encryption, app operability, and authentication are established factors contributing to data breaches [7].

Several studies have highlighted the connection between patients' awareness and the risk of data breaches [7-9]. End-users have an obligation for the security and privacy of their data, to be maintained [4,10]. As the main stakeholders of the healthcare system, patients have a contractual relationship with healthcare providers as the latter is expected to ensure the safety and confidentiality of patients' health information confidential. While mhealth providers are aware of the security measures, privacy, and confidentiality related to patient's health data, the latter appears to lag in these

vital aspects [4,10].

In Saudi Arabia's context, the healthcare economy is fast growing owing to the digitisation of the sector [11]. This advancement in healthcare service delivery is related to the nation’s high penetration rate of smartphones, the Internet, and social networking usage in the Arabic Gulf. Recent statistics indicate that smartphone and mobile phone users in the KSA will increase from 21.87 and 23.77 million in 2018 to 24.02 and 30.0 million in 2025, respectively [11]. In line with the increasing population of smartphone users, Saudi Arabia has implemented several mhealth apps according to its Vision 2030 goals [12]. As part of the nation’s goals, the implementation of the digital transformation plan for private and public health sectors commenced in 2017 [13]. The Saudi Ministry of Health (MOH) has specifically created several mobile apps to facilitate administrative protocols for users and patients to allow them to receive medical consultations and update their medications [12,14].

Nevertheless, the adoption of the mhealth app in Saudi Arabia has yet to achieve the expected benchmark [13]. Issues relating to safety, privacy, and confidentiality of information shared via mHealth apps that are connected to CICs have been reported in recent studies [11,15]. These challenges might contribute to the low adoption rate among end-users and patients. Nevertheless, this can only be established by understanding their awareness of the raised issues. For instance, significant security and privacy issues were reported in previous studies that could lead to data breaches with severe social, legal, and financial consequences [11,15]. Aljedaani *et al*. [15] presented empirical evidence that most end-users of mhealth apps were unaware of the current security features provided. A recent study within the context of mhealth apps in Saudi Arabia reported that only a few participants were aware of adverse drug reactions and denied receiving prior education and attending events relating to such mhealth apps [16].

Another issue regarding existing literature on mhealth apps in the KSA is that most previous studies have focused more on healthcare professionals, whereas patients’ perspectives have received little attention [15]. Both developers' and users’ perspectives need to be balanced to ensure that mhealth apps achieve their targeted goals in enhancing healthcare service delivery. However, no qualitative analysis of users’ awareness and perspectives regarding data privacy, confidentiality, and security has been attempted in Saudi Arabia. In addition, there is data paucity regarding users’ awareness of privacy concerns and the resulting impact on the acceptance of mHealth apps, especially in the Saudi context. Such information is pertinent in addressing users’ needs and developing patient-friendly mHealth apps in the KSA. This article presents a study protocol for a mixed-method analysis of patients’ and stakeholders’ perspectives regarding the privacy, confidentiality, and security of data collected via mHealth apps in Saudi Arabia. The study scope, theoretical background, and research hypotheses are presented in the next section.

Scope

The scope of the present study is precise in terms of end-users’ awareness of the security, privacy, and confidentiality regarding clinical mhealth apps, such as patient management systems that handle highly sensitive health-critical data and personal information. This study focuses on end-user perspectives, specifically their awareness of the security, privacy, and confidentiality of information collected via mhealth apps. This study will provide an in-depth view of end-users' security awareness by evaluating their current knowledge of existing security features provided by mhealth apps available in the country. Additionally, the relationship between end-users'/patients’ security awareness and their socio-demographic characteristics will be elucidated while identifying specific security features that may enhance end-users’ confidence in using mhealth apps. The findings will assist in benchmarking the effectiveness of mhealth apps' security features that need to be considered by developers while engineering the existing or next generation of mhealth apps in the context of Saudi Arabia. These may improve mhealth app adoption in Saudi healthcare management.

Theoretical Framework

A review of the current literature depicts extensive usage of different technology acceptance theories relating to the adoption of advanced healthcare systems, such as the Technology Acceptance Model (TAM), the theory of Reasoned Action (TRA), health information management, and information assurance and security ethical behaviour [17]. The TAM is a widely deplored model for investigating technology acceptance in information systems, such as healthcare systems, due to its understandability and simplicity [18]. The proponents of TAM argued that the key to promoting use is to increase the acceptance of information technology, which is measurable based on an individual's future intention to use [19].

Closely related to TAM is the theory of reasoned action (TRA), which encompasses a psychological approach that reflects how individuals' belief systems mediate human behaviour. TRA posits that an individual's behavioural intention (BI) to use a system is determined by the individual's subjective norms and attitude associated with the behaviour [19]. Fernandez-Aleman *et al*. [20] assessed the psychosociocultural (PSC) framework and some other socio-demographic features (gender, age, and experience) in their research and they advocated for better security awareness training to promote good security practices.

Another approach utilised in a previous study was the combination of the protection motivation theory (PMT) and the theory of planned behaviour (TPB) [21]. These theories were used to determine whether security practices were affected by security awareness, experience, and information policy. Whereas the TPB depends on subjective norms, attitudes, and perceived behaviours predicting human behaviour [22], the PMT emphasises the ability to protect oneself from threats based on the perceived likelihood of occurrence or vulnerability, `perceived severity of a threat, perceived self-efficacy and the impact of recommended preventive measures [21].

Thus, various theories could be adopted in evaluating security practices and perspectives of users regarding e-health and mHealth in the Saudi context. Given that socio-demographic characteristics influence healthcare security practices and psychological factors, this study attempts to propose the PSC framework to facilitate a holistic approach toward elucidating users' characteristics and antecedents for using mHealth apps in Saudi Arabia, as well as their views on data privacy, security, and confidentiality. Since users' acceptance levels, awareness and antecedents will be assessed in this study, the TAM theory will be considered in developing the conceptual framework.

Research Hypotheses

This study proposes awareness of data privacy, security, and confidentiality as a predictor of behavioural intention towards using mHealth apps among the Saudi population. The literature posits that users' awareness of data privacy makes them circumspect about adopting technology and sharing their personal information [4,6]. Users' perspectives and concern about data privacy of health information may influence their avoidance of using specific healthcare services, mHealth in the present context [9]. Previous research revealed that the failure to mitigate customers' privacy coseverely impactmpacts on the customers' behaviour and attitude towards healthcare services [23,24]. Mukherjee and Nath [23] also found that security to privacy combined with shared values was positively associated with customers' behavioural intention. The present study aligns with the argument that privacy, security, and confidentiality concerns are related to end-users or patients' assessment of lack of reliance on mHealth apps, especially relating to sharing their personal data. Hence, based on the aforementioned arguments, the following hypotheses are proposed:

H1(a): Behavioural intention to use mHealth apps connected to CICs is associated with users' awareness level of data privacy, security, and confidentiality issues.

H1(b): Socio-demographic factors (i.e., gender, age, job type, income level, location, and educational qualification) are associated with users' awareness level of data privacy, security, and confidentiality issues.

In terms of acceptance of mHealth apps among the Saudi population, this study attempts to utilise the TAM in deriving the research hypotheses. The two key components of TAM are perceived ease of use (PEOU) and perceived usefulness (PU), and they are believed to influence users' behavioural intentions (BI) [24]. Despite the extensive research on data privacy and security in different environments and contexts, only a few studies considered the effects of privacy concerns on PU and PEOU [25]. In fact, no study in the literature focused on these aspects in users' or patients' adoption of mHealth apps. A study reported that higher privacy and security concerns played a negative mediating role in the association between users' perceived risk and attitude [25]. Therefore, it is plausible to predict that patients or end-users will not find usefulness in technology with a high risk of invading their privacy. People are more likely to direct more effort towards monitoring, especially when they perceive that their data privacy is threatened while using any service. Thus, privacy and security concerns might decrease individuals' perceived ease of use and usefulness for any service, including the use of mHealth apps. Based on these arguments, the following hypotheses are proposed:

H2(a). Privacy, security, and confidentiality concern is negatively associated with the Perceived usefulness (PU) of using mHealth apps.

H2(b). Privacy, security, and confidentiality concern is negatively associated with Perceived ease of use (PEOU) to use mHealth apps.

Research Objectives

i. To explore patients' and stakeholders' awareness level and perspectives on issues relating to the privacy, security, and confidentiality of data collected via mHealth apps in Saudi Arabia.
ii. To determine the association between behavioural intention to use mHealth apps and users' awareness level of data privacy, security, and confidentiality issues.
iii. To determine the association between patients' socio-demographic factors and concerns regarding data privacy, security, and confidentiality issues.
iv. To determine the association between patients' perceived usefulness (PU) of mHealth apps and concerns regarding data privacy, security, and confidentiality.
v. To determine the association between patients' perceived ease of use (PEOU) of mHealth apps and concerns regarding data privacy, security, and confidentiality.
vi. To propose initiatives for the Saudi government to improve Saudi users/patients' adoption of mhealth apps and address the concerns relating to data privacy, security, and confidentiality.

Research Questions

In line with the research objectives, this study aims to answer the following questions:

i. What is the patient awareness level of data confidentiality, privacy, and security issues of mhealth apps in Saudi Arabia?
ii. Is there any relationship between behavioural intention to use mHealth apps and users' awareness level of data privacy, security, and confidentiality issues?
iii. Is there any relationship between patients' socio-demographic factors and concerns regarding data privacy, security, and confidentiality issues?
iv. Is there any relationship between patients' PU of mHealth apps and concerns regarding data privacy, security, and confidentiality?
v. Is there any relationship between patients' PEOU of mHealth apps and concerns regarding data privacy, security, and confidentiality?
vi. What are the perspectives of patients and stakeholders regarding the privacy, security, and confidentiality of data collected via mHealth apps?

Methods

Study Area and study design

There are a total of 13 provinces in Saudi Arabia, namely, Riyadh, Madinah, Mecca, Tabuk, Najran, Hall, Northern, Eastern, Al Jouf, Asir, Qassim, Jazan, and Al Baha. However, this study will focus on regions encompassing hospitals with state of art facilities and currently using mHealth apps for patient management. mHealth users from the identified provinces will be considered during the recruitment process, irrespective of their current place of work or occupation. Hence, mHealth users in the health, service, educational, and industrial sectors will be recruited into the study as long as they fufill the inclusion criteria. These study sites were selected since they are Saudi Arabia's fastest-growing medical complexes and have implemented mHealth apps that connect patients straight to CISs. Given the high number of patients and users of mHealth apps in the aforementioned provinces, including the availability of clinicians and healthcare providers who are experienced in mHealth apps connected to CISs, these study sites will enable the researcher to gather the required data to execute the research objectives.

A mixed-method approach of qualitative and quantitative methods will be used in this study. This study will be exploratory due to the data paucity on the aforementioned research topics in the Saudi context. Hence, mixed methods will enable the researcher to develop a broad breadth of the topic. The mixed-method approach ensures convergence and correspondence of results drawn from different method [26,27].

Qualitative data will be collected via a structured interview involving stakeholders of mHealth apps in Saudi Arabia while the quantitative phase will involve patients either currently using mHealth apps or not but seeking health services from healthcare facilities in Saudi Arabia. For the quantitative phase, a structured survey (questionnaire) will be developed, validated, and pilot-tested before conducting the actual survey. Thus, the first to fifth research questions will be answered in the quantitative phase while qualitative data will be collected for the sixth research question. Given that different participants will be enrolled for the quantitative and qualitative parts, both phases will be conducted concurrently.

Study population

The study population and unit of analysis in this study encompasses all the patients and other stakeholders that fulfil the inclusion criteria. Meanwhile, the target population will be mHealth app users actively seeking health services from healthcare institutions, as well as other stakeholders such as app developers, healthcare professionals, and policy makers in Saudi Arabia’s health sector.

Inclusion and exclusion criteria

Certain inclusion and exclusion criteria will be considered in this study for respondents’ recruitment. The target participants will be mHealth app users and stakeholders and aged 18 years and above. For the patients, they must be actively seeking health services, currently visiting any hospital in any Saudi Arabia’s province, and must have a basic understanding of the functions of mHealth apps. Meanwhile, individuals less than 18 years old, lacking the basic knowledge of mHealth apps, and not currently visiting any hospital in the provinces will be excluded from this study. On the other hand, the stakeholders have to be either healthcare professionals, mHealth app developers or policy makers who are experienced with mHealth apps. Such knowledge will assist the researcher in elucidating patients’ and stakeholders’ perspectives regarding data confidentiality, privacy, and security issues in the usage of mHealth apps.

Sample size calculation and sampling technique

The sample size for the quantitative phase will be estimated based on the estimated total population

of mHealth app users in the study locations, a confidence interval of 95%, a precision error of 5%, and estimates from previous related studies on the adoption rate of mHealth apps in Saudi Arabia and other countries in the Middle East. Specifically, the sample size will be estimated by utilising the formula for analytical and cohort studies presented below:

$$n' = \frac{\left[z_{1-\alpha/2}\sqrt{2\acute{P}\left(1-\acute{P}\right)} + z_{1-\beta}\sqrt{P_1\left(1-P_1\right)+P_2\left(1-P_2\right)}\right]^2}{¿¿}$$

$$n = \frac{n'}{4}\left(1+\sqrt{1+\frac{2(2)}{n'\left(P_2-P_1\right)}}\right)^2$$

Where,
n = Sample size
Z1 – α/2 = Z statistic for 95% confidence level = 1.96
Z1-β = Z statistic for 90% power = 1.28
P_1 = Proportion of participants with satisfactory accessibility and receptiveness levels toward counselling in one group
P_2 = Proportion of participants with satisfactory accessibility and receptiveness levels toward counselling in one group
P_1 and P_2 will be obtained from previous studies conducted in Saudi Arabia or other countries in the Middle East reporting the proportions of participants adopting mHealth apps or being aware of data privacy, security or confidentiality issues. The obtained values will be substituted into the equation to calculate the required sample size (n). A non-response rate of 20% will also be considered before deciding on the final sample size. The probability proportionate to size (PPS) method will be utilised to allocate sample size for each selected province to facilitate proportionate distribution of patients and users of mHealth apps. Thereafter, a convenience sampling technique will be used to obtain the required number of participants from each region. Meanwhile, purposive sampling will be utilised in selecting the provinces as mentioned in the study design and study area.

Qualitative phase: Study instrument and Interview Session

A semi-structured interview will be developed in the qualitative phase. The interview session involves patients, developers of mHealth apps, and healthcare professionals. Questions in the interview session will be synthesised based on an in-depth review of previous literature and discussion between the researchers. Previous studies that deployed interviews or focus group discussions will be reviewed [4, 24], followed by selecting and modifying the topics relevant to the present study and the Saudi context. Overall, the questions will focus on (1) how to improve patients' awareness of data security, privacy, and confidentiality, (2) feedback on the current mHealth apps in terms of data security, privacy, and confidentiality, (3) the features that might improve data security, privacy, and confidentiality of mHealth apps connected to CICs. The interview guide will enable the participants to share their experiences of using mHealth apps and their concerns regarding data security, privacy, and confidentiality.
The interview will be performed by a trained enumerator and conducted in English or Arabic depending on the participant preference. The interview is expected to last for 10-20 minutes and the location would be the hospitals for the patients, whereas the stakeholders will be interviewed based on their preferred locations. The relevant authorities and personnel in the hospitals will be contacted and briefly informed regarding the research objectives and methodology. Upon receiving approval from hospitals, potential participants will be approached during their visits and their consent to participate in the study will be sought. The same method will be used in recruiting the stakeholders from the respective industries. A snowball method will also be employed whereby participants would

be informed to nominate other potential patients or stakeholders that will be willing to take part in the study. With participants' permission, a voice recorder will be available during the interview session. Different participants will be recruited in the qualitative and quantitative phases.

Quantitative phase: Instrument development and Administration

Questionnaire development comprises designing, directing, and compiling the items for assessing or measuring various constructs in a given survey [28]. A multi-dimensional approach was applied to develop the instrument to be used in this study. The approach entailed findings gleaned from previous related research, modification of instruments utilised in prior studies and discussion among the researchers. The structured questionnaire was designed in two broad parts; Part 1 and 2. Part 1 contained demographic details such as age, gender, marital status, occupation, income level, education level, current health app usage, and frequency of mobile App use. As discussed in the previous section, participants' socio-demographic factors are crucial in understanding the adoption of a new healthcare technology such as mHealth apps. These socio-demographic factors were selected in this study based on previous research demonstrating their relevance in the adoption of mHealth and their association with security and privacy issues in the Saudi context [15]. The second part of the questionnaire (Part 2) consists of six sections. The first section was designed to gather information on patients' awareness of mobile health apps connected to CISs. A total of five items **(Q1-Q5)** were adopted from previous research conducted by AlJedaani et al. [15] with slight modifications to suit the present study context. The questions emphasize patients' awareness of access to their personal data, installation of trackers, and their self-reported awareness level of data privacy and security.

The second section focuses on patients' privacy concerns about mHealth apps. A total of eight **(Q6-Q13)** items were utilised in this section as described by Dhagarra et al. [24] with slight modifications. The initial three items seek patients' concerns regarding the extent of information requested and those collected by health centres. Meanwhile, the remaining items emphasised concerns relating to access from authorized persons, non-accurate storage of patient data, and measures taken to ensure data privacy.

The third section is designed to assess patients' concerns about data confidentiality in mHealth apps. A total of six **(Q14-Q19)** items are utilised in this section as described by Al-Jedaani et al. [15]. The first and second items seek patients' concerns relating to sharing confidential data, whereas the remaining three items focus on actions taken to ensure the confidentiality of data shared via mhealth apps.

The fourth section focuses on data security, comprising seven items **(Q20 to Q27)**. These items were adopted from the studies conducted by Al-Jedaani et al. [15], Zhou et al. [29], and Zhou et al. [4]. Likewise, the items include actions to ensure data security, such as password settings, security policies and settings, encryption functions, and user authentication.

The perceived usefulness/utility of mobile health apps was investigated in the fifth section, comprising four items **(Q28-31)** to document patients' responses to the expected effects of mhealth apps on productivity, performance, effectiveness, and accessibility to healthcare services. Meanwhile, perceived ease of use was evaluated in the sixth section using six items **(Q32-Q37)** adopted from the sources reported for perceived utility. The last section contains three items **(Q38-Q40)** adapted from Dhagarra et al. [24] to assess patients' behavioural intentions.

Finally, the questionnaire will be translated from English to Arabic by two experienced translators. Upon completing the translation process, both versions of the questionnaire will be subjected to pilot testing to assess the validity and reliability of the instrument. Findings from the experts' opinions and pilot testing will be employed to prevent potential ceiling and floor effects from the questionnaire items that may affect accurate data interpretation. The developed questionnaire (see supplementary

file) will be distributed either online (i.e., Google Forms and Qualtrics) or self-administered to selected patients and users of mHealth apps in Saudi Arabia. The method of administrating the questionnaire will depend on the participants' preferences. Data obtained from the quantitative and qualitative approaches will be combined to provide a more robust assessment of the study (Figure 1).

Ethical consideration

Ethical approval is vital for this study as the researcher will recruit patients and users of mHealth apps. The ethical approval for this research has been obtained from the Biomedical and Scientific Research Ethics Committee, University of Warwick and the Medical Research & Ethics Committee Ministry of Health in the KSA. Participation will be anonymous to ensure that participants' confidentiality of the participants maintained throughout the research. No identifying details will be obtained from the participants during the research process. The researcher will also state the confidentiality of all information provided by the participants. The participants will be informed that they can decide to withdraw from the study at any time without any penalty. All collected data will be stored on a personal computer with a secure password and only accessible to authorised parties (the supervisory team and the researcher).

Management and Quality Control Measures

Participants' anonymity will be protected in this research and all data will be kept confidential without revealing the participants' identities. When submitting the results to sponsors or regulatory institutions, all participants' clinical records will be represented using a coding system, which will only be accessible by the researcher. Each participant will be given two copies of consent forms signed by both parties. All data files will be stored in a single folder in a secured location.

This study does not expose the participants to any risk and no personal expenses will be incurred either during the interview or filling up the survey. In addition, participation is not associated with any financial gain or incentives. All expenses will be borne from the research budget. Participation is voluntary and there are no implications for the participants' health upon deciding not to take part in the study. Participants can also demand to terminate their participation irrespective of time, without any consequences to their care at the hospitals. The research findings will be published in journal articles and presented at conferences or meetings; nevertheless, participants' identities will remain confidential.

Several methodological resources including mixed-method study design, inclusion criteria, and random sampling will be employed to ensure quality control and reduce bias when gathering the data. The interviews, and data collection during the quantitative phase will be completed by trained enumerators. Quality control will be further evaluated by assessing the enumerators periodically to ensure the survey protocol is adhered to. The retrieved questionnaire will be assessed in terms of data completeness and quality.

Data Analysis

The qualitative data will be transcribed, coded and analysed thematically using NVivo (Version 12), leading to the emergence of themes and sub-themes. A reliability analysis based on Cronbach alpha will be performed to assess the internal consistency of the questionnaire. The items with a minimum Cronbach alpha value of 0.7l will be considered reliable and acceptable. Descriptive statistics will be used to summarise the participants' background information, and other sections in the questionnaire items measured in scale will be checked for normality using the Smirnov-Kolmogorov test and presented in mean (± standard deviation) or median (± interquartile range) depending on the normality results. The association between the variables will be determined statistically using simple and multiple linear regression models. Both SPSS version 25 and smart-PLS will be used accordingly. Aligning with the present study, measurement and structural models in PLS-SEM will

be constructed to test the research hypotheses. PLS-SEM is chosen as it aligns with the predictive-oriented objectives of this study.

Timeline

The participants for the qualitative study have been recruited, and the interviews will be completed by November 2023. Participant recruitment for the quantitative phase is being performed currently and is expected to be completed by May 2024. Data analysis will be performed by June 2024 and the research will be completed by August 2024.

Results

The ethical approval for this research has been obtained from the Biomedical and Scientific Research Ethics Committee, University of Warwick and the Medical Research & Ethics Committee Ministry of Health, Saudi Arabia. The qualitative phase is ongoing and 15 participants have been interviewed. The interviews for the remaining 10 participants will be completed by 25 November 2023. Preliminary thematic analysis is still ongoing. Meanwhile, the quantitative phase is currently ongoing as well with 150 participants providing signed and informed consent to participate in the study. The data collection for the quantitative part is expected to be completed by May 2024. Data analysis will be performed by June 2024 and the research will be completed by August 2024.

Discussion

Expected Findings

Research has shown that patients' awareness level of mHealth apps is a strong predictor of adopting the technology for health management [4,30]. However, there is a paucity of research focusing on patients' concerns regarding data privacy and data security and the influence on mHealth app usage. Therefore, the first objective of this study is to empirically assess patients' awareness and perception of issues relating to the privacy, security, and confidentiality of data collected via mHealth Apps in Saudi Arabia.

The findings will assist the relevant stakeholders in identifying the factors contributing to low awareness levels about data security and privacy, as well as the areas requiring utmost attention. Since this study also involves qualitative assessment, the underlying events leading to discordant perspectives on mHealth apps can also be gleaned from the analysis. For instance, users who are more aware of mHealth apps, healthcare providers' role during the data collection, and the importance of using collected patient data strictly for medical purposes may demonstrate more concerns regarding data security and privacy.

Saudi Arabia's government has intensified efforts to improve the adoption and usage of e-health and telemedicine modalities by organising awareness campaigns and investing in the country's healthcare sector [12]. Such strategies might positively impact the stakeholders and influence behavioural intention to use the advanced health technologies. Nonetheless, no specific approaches have been taken to explore users' and healthcare professionals' perspectives regarding the security and privacy of data collected via such apps. The results from this study will elucidate these aforementioned gaps in knowledge.

Four broad research hypotheses will be tested in this study, based on the constructs in TAM (PEOU, PU, and behavioural intention) and patients' awareness and concerns relating to data privacy, security, and confidentiality. Previous studies reported that users' awareness of data privacy triggered their intention to adopt the technology and share their personal information **[4, 31]**. The usage of specific healthcare services, including mHealth, may be shaped by users' perspectives and concerns about data privacy of health information [9]. However, most of these studies were empirical and not supported by theoretical frameworks.

In this study, we hypothesised that PU and PEOU will directly influence users' concerns about data security, privacy, and confidentiality. PEOU entails the ease of operating the technology in question, understanding the features, and the support provided to address any difficulty faced. We expect at least one or more of the hypotheses to be supported, reflecting that users' PU or PEOU to use mHealth apps will increase once their concerns about data security, privacy, and confidentiality are addressed. In other words, one approach to address users' concerns regarding data security is ensuring they can easily navigate the technology and access the security features. These expected findings are consistent with the reports from previous studies on various approaches to improve the

adoption and uptake of mHealth apps [32,33].
Specific themes and sub-themes will emerge from the qualitative phase and be aggregated with the empirical findings from the quantitative data. Therefore, our study will assist in elucidating the events that shape participants' concerns regarding data privacy, security, and confidentiality. Diverse perspectives will be gleaned since this study encompasses stakeholders, healthcare professionals, and patients. Past research demonstrated that severe consequences on users' behaviour and attitude towards healthcare services may arise from failure to address issues relating to data security and privacy violations [23,24]. Likewise, a recent review by Nurgalieva et al. [34] also revealed that low levels of security and privacy are the main drive for declining uptake of mHealth apps among the target audience. The expected themes in the present study may also include negative perceptions, fear of data breaches, and failure to address issues relating to data security and privacy violations.
We also attempt to identify the association between participants' demographic attributes and concerns regarding the privacy and security of mHealth apps. A previous study found that married patients demonstrated higher information security and privacy concerns and desired more stringent security protection than single patients [4]. In addition, users who earned less than 10, 000 USD annually exhibited the weakest concerns about the privacy and security provided by mHealth apps. Apart from these factors, we expected attributes such as age and educational background to influence concerns regarding the privacy and security of mHealth apps in Saudi Arabia's context. For instance, users who are highly educated are more likely to understand and update their knowledge of data security features available in mHealth apps. This group of respondents is also more inclined to inform the app developer if any data privacy or confidentiality issue is experienced. Younger patients or users are the predominant users of various social media platforms with security notifications and authentication, which increases the risk of exposure to events relating to data breaches. Besides, they spend more time on their smartphones than the older population. These events may culminate in greater concerns regarding data privacy and security of mHealth apps.

Implications

This study has important implications for mHealth app developers, end-users, and the healthcare system in Saudi Arabia. The security and adoption of mhealth systems could be effectively strengthened if both developers' and patients' perspectives of mhealth apps are aligned [35]. Mhealth developers can use the research findings to identify the specific security features that require urgent adjustment to ensure the safety of patient health information, the delivery of healthcare service efficiently, and maintain the balance between security and usability. More importantly, the developers will gain direct information from the main stakeholders in mhealth apps: patients and end-users. On the other hand, patients will be able to share their views regarding the security, privacy, and confidentiality of sharing their health data via mhealth apps. This in turn could elicit vital adjustments that will enhance both the security and usability of such apps and other numerous advantages associated with the connection of mhealth apps to CICs.
Saudi Arabia has also introduced several mhealth apps in order to enhance healthcare service delivery, aligning with its Vision 2030 goals [12]. The findings from this study will reflect underlining issues relating to patients' and users' awareness of security and privacy features provided in mhealth apps implemented by the Saudi government. Hence, the research outcomes might reveal certain factors contributing to the present low adoption rate of mhealth apps among the population. Necessary adjustments in terms of decision-making, policies, and investments could be performed to ensure that mhealth apps align with Vision 2030 goals, particularly in public health.

Limitations

Despite employing a mixed-method approach in this study, certain methodological limitations need to be acknowledged. The inclusion and exclusion criteria employed in selecting the study subjects

might exclude potential participants with pertinent information on the research topics. Furthermore, only patients will be recruited for the survey and the use of survey instruments has its limitations in terms of response bias. Respondents might also be unwilling to provide in-depth information about the questions during the interview. These limitations may affect the generalisability of the results. Lastly, this study is a cross-sectional design and the findings will only depict the association between the studied variables, which entails PEOU, PU, and behavioural intention to use mhealth apps, as well as awareness and concerns regarding data privacy, security, and confidentiality. In other words, no causal relationships would be inferred. Notwithstanding, the strengths of this study stem from the dearth of information on the research topic in Saudi Arabia's context, including the data paucity on studies employing mixed methods to bridge the knowledge gap.

Conclusion

Accumulated evidence reflects the knowledge gap on the antecedents of patients' awareness and concerns regarding the privacy, security, and confidentiality of data collected via mHealth apps in Saudi Arabia. Likewise, the perspectives of stakeholders and healthcare professionals toward the aforementioned issues are not fully understood. Given the rising usage of smartphones, huge investment in mHealth apps, and the campaign to improve the usage of advanced healthcare systems in Saudi Arabia, this research will be pertinent in elucidating a vital aspect that may jeopardise these targeted goals Policymakers and relevant bodies can use the findings to implement a model that will enhance the adoption of mHealth apps and address issues relating to the privacy, security, and confidentiality of data collected via mHealth apps.

Data availability

Upon completing this study, the important data underlying the findings will be described in the manuscript at the time of publication. Additional data will also be provided in a supporting document.

Authors' Contributions

All authors have made substantial contributions to the work presented in this manuscript.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare that they have no conflict of interest.

References

1. Chen, J. *et al.* (2017) 'The use of smartphone health apps and other mobile health (mHealth) technologies in dietetic practise: a three country study', *Journal of Human Nutrition and Dietetics*, 30(4), pp. 439–452. doi: 10.1111/jhn.12446.
2. Hussain, M. *et al.* (2018) 'Conceptual framework for the security of mobile health applications on Android platform', *Telematics and Informatics*. Elsevier, 35(5), pp. 1335–1354. doi: 10.1016/j.tele.2018.03.005.
3. Fagherazzi, G., Goetzinger, C., Rashid, M. A., Aguayo, G. A. & Huiart, L. (2020) Digital health strategies to fight COVID-19 worldwide: challenges, recommendations, and a call for papers. J. Med. Internet Res. 22, e19284.
4. Zhou, L. *et al.* (2019) 'Barriers to and facilitators of the use of mobile health apps from a

security perspective: Mixed-methods study', *JMIR Mhealth Uhealth*, 7(4), p. e11223. doi: 10.2196/11223.

5. Kao, C. K. and Liebovitz, D. M. (2017) 'Consumer Mobile Health Apps: Current State, Barriers, and Future Directions', *Clinical Informatics in Physiatry*. American Academy of Physical Medicine and Rehabilitation, 9(5S), pp. S106–S115. doi: 10.1016/j.pmrj.2017.02.018.
6. Li, J., Silvera-Tawil, D., Varnfield, M., Hussain, M. S., & Math, V. (2021). Users' Perceptions Toward mHealth Technologies for Health and Well-being Monitoring in Pregnancy Care: Qualitative Interview Study. *JMIR formative research*, *5*(12), e28628. https://doi.org/10.2196/28628
7. S. Bhuyan, S. *et al.* (2017) 'Privacy and security issues in mobile health: Current research and future directions', *Health Policy and Technology*. Elsevier Ltd, 6(2), pp. 188–191. doi: 10.1016/j.hlpt.2017.01.004.
8. Sampat, B. H. and Prabhakar, B. (2017) 'Privacy Risks and Security Threats in mHealth apps', *Journal of International Technology and Information Management*, 26(4), pp. 126–153.
9. Asiri, Eman, Hanan Asiri, and Mowafa Househ. 'Exploring the Concepts of Privacy and the Sharing of Sensitive Health Information'. In *Integrating Information Technology and Management for Quality of Care*, 161–64. IOS Press, 2014. https://doi.org/10.3233/978-1-61499-423-7-161.
10. Esposito, M., Minutolo, A., Megna, R., Forastiere, M., Magliulo, M., & De Pietro, G. (2018). A smart mobile, self-configuring, context-aware architecture for personal health monitoring. *Engineering Applications of Artificial Intelligence*, *67*, 136–156. https://doi.org/10.1016/j.engappai.2017.09.019
11. Alanzi T. mHealth for diabetes self-management in the Kingdom of Saudi Arabia: barriers and solutions. J Multidiscip Healthc. 2018 Oct 8;11:535-546. doi: 10.2147/JMDH.S174198. PMID: 30349285; PMCID: PMC6183657.
12. Young, Yuchi, Amani Alharthy, and Akiko S. Hosler. 'Transformation of Saudi Arabia's Health System and Its Impact on Population Health: What Can the USA Learn?' *Saudi Journal of Health Systems Research* 1, no. 3 (20 August 2021): 93–102. https://doi.org/10.1159/000517488.
13. Aljohani, Nasser, and Daniel Chandran. 'The Adoption of Mobile Health Applications by Patients in Developing Countries: A Systematic Review'. *International Journal of Advanced Computer Science and Applications (IJACSA)*12, no. 4 (56/01 2021). https://doi.org/10.14569/IJACSA.2021.0120403.
14. Hassounah, M., Raheel, H., and Alhefzi, M. 2020. "Digital Response During the Covid-19 Pandemic in Saudi Arabia," Journal of Medical Internet Research (22:9), p. e19338.
15. Aljedaani, Bakheet, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. 'End-Users' Knowledge and Perception about Security of Clinical Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers'. *Journal of Systems and Software* 195 (January 2023): 111519. https://doi.org/10.1016/j.jss.2022.111519.
16. Kassem LM, Alhabib B, Alzunaydi K, Farooqui M. Understanding Patient Needs Regarding Adverse Drug Reaction Reporting Smartphone Applications: A Qualitative Insight from Saudi Arabia. Int J Environ Res Public Health. 2021 Apr 7;18(8):3862. doi: 10.3390/ijerph18083862. PMID: 33917014; PMCID: PMC8067764.
17. Liu, Y., Lu, X., Zhao, G., Li, C., & Shi, J. (2022). Adoption of mobile health services using the unified theory of acceptance and use of technology model: Self-efficacy and privacy concerns. *Frontiers in Psychology*, *13*, 944976. https://doi.org/10.3389/fpsyg.2022.944976
18. Rajak, M., & Shaw, K. (2021). An extension of technology acceptance model for mHealth user adoption. *Technology in Society*, *67*, 101800.

https://doi.org/10.1016/j.techsoc.2021.101800

19. Lewis TL, Wyatt JC. (2014). mHealth and mobile medical Apps: a framework to assess risk and promote safer use. *J Med Internet Res,* **16**: e210 [PMID: 25223398 DOI: 10.2196/jmir.3133]
20. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. J Biomed Inform. 2013 Jun;46(3):541-62. doi: 10.1016/j.jbi.2012.12.003. Epub 2013 Jan 8. PMID: 23305810.
21. Safa, Nader Sohrabi, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 'Information Security Conscious Care Behaviour Formation in Organizations'. *Computers & Security* 53 (September 2015): 65–78. https://doi.org/10.1016/j.cose.2015.05.012.
22. Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior [1]. *Journal of Applied Social Psychology*, *32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x
23. Mukherjee, Avinandan, and Prithwiraj Nath. 'Role of Electronic Trust in Online Retailing: A Re-examination of the Commitment-trust Theory'. Edited by David C. Arnott and David Wilson. *European Journal of Marketing* 41, no. 9/10 (1 January 2007): 1173–1202. https://doi.org/10.1108/03090560710773390.
24. Dhagarra, Devendra, Mohit Goswami, and Gopal Kumar. 'Impact of Trust and Privacy Concerns on Technology Acceptance in Healthcare: An Indian Perspective'. *International Journal of Medical Informatics* 141 (September 2020): 104164. https://doi.org/10.1016/j.ijmedinf.2020.104164.
25. Andrews, L., Gajanayake, R., and Sahama, T. (2014). The Australian general public's perceptions of having a personally controlled electronic health record (PCEHR). *Int. J. Med. Inform.* 83, 889–900. doi: 10.1016/j.ijmedinf.2014.08.002
26. Schoonenboom, J., Johnson, R.B. How to Construct a Mixed Methods Research Design. *Köln Z Soziol* **69** (Suppl 2), 107–131 (2017). https://doi.org/10.1007/s11577-017-0454-1
27. Regnault, A., Willgoss, T., Barbic, S. *et al.* Towards the use of mixed methods inquiry as best practice in health outcomes research. *J Patient Rep Outcomes* **2**, 19 (2018). https://doi.org/10.1186/s41687-018-0043-8
28. Cooper, D. and Schindler, P. (2011) Business Research Methods. 11th Edition, McGraw Hill, Boston.
29. Zhou, L. *et al.* (2018) 'A mobile app for assisting users to make informed selections in security settings for protecting personal health data: Development and feasibility study', *JMIR Mhealth Uhealth*, 6(12), p. e11210. doi: 10.2196/11210.
30. Natsiavas, P. *et al.* (2019) 'Citizen perspectives on cross-border eHealth data exchange: A European survey', in (Eds.), L. O.-M. and B. S. (ed.) *MEDINFO 2019: Health and Wellbeing e-Networks for All*. IOS Press, pp. 719–723. doi: 10.3233/SHTI190317.
31. Kayyali R, Peletidi A, Ismail M, Hashim Z, Bandeira P, Bonnah J. Awareness and Use of mHealth Apps: A Study from England. Pharmacy (Basel). 2017 Jun 14;5(2):33. doi: 10.3390/pharmacy5020033. PMID: 28970445; PMCID: PMC5597158.
32. Dang, Y., Guo, S., Guo, X., Wang, M., & Xie, K. (2021). Privacy Concerns About Health Information Disclosure in Mobile Health: Questionnaire Study Investigating the Moderation Effect of Social Support. *JMIR mHealth and uHealth*, *9*(2), e19594. https://doi.org/10.2196/19594
33. Zhang, D., Lim, J., Zhou, L., & Dahl, A. A. (2021). Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study. *JMIR mental health*, *8*(12), e31633. https://doi.org/10.2196/31633

34. Nurgalieva, L., O'callaghan, D., Doherty G. (2016). Security And Privacy Of Mhealth Applications: A Scoping Review. IEEE Access, 4

35. Atienza AA, Zarcadoolas C, Vaughon W, Hughes P, Patel V, Chou WS, (2015). Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. J Health Commun, Apr;20(6):673-679. [doi: 10.1080/10810730.2015.1018560]

Supplementary Files

Untitled.
URL: http://asset.jmir.pub/assets/457329f5bae1d68a2e0d68da1ec06b3a.docx

Untitled.
URL: http://asset.jmir.pub/assets/f8040f30165270ea5674972698b11093.docx

Untitled.
URL: http://asset.jmir.pub/assets/1cf2bd5bd8c3ebf2d64a76d37283dc61.docx

Related publication(s) - for reviewers eyes onlies