

A systematic review of patients' perspectives on data confidentiality, privacy, and security of mobile health applications

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

Submitted to: Journal of Medical Internet Research
on: July 10, 2023

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on its website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressly prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

Original Manuscript.....	5
---------------------------------	----------

Preprint
JMIR Publications

A systematic review of patients' perspectives on data confidentiality, privacy, and security of mobile health applications

Nasser Alhammad^{1,2} MSc; Mohannad Alajlani¹ PhD; Alaa Abd-alrazaq³ PhD; Gregory Epiphaniou¹ PhD; Theodoros Arvanitis⁴ PhD

¹University of Warwick Coventry GB

²Saudi Electronic University Jeddah SA

³AI Center for Precision Health, Weill Cornell Medicine Doha QA

⁴University of Birmingham Birmingham GB

Corresponding Author:

Nasser Alhammad MSc

University of Warwick

Institute of Digital Healthcare, WMG

Coventry

GB

Abstract

Background: Mobile Health Applications (mHealth apps) have the potential to enhance healthcare service delivery. However, concerns regarding patients' confidentiality, privacy, and security consistently affect the adoption of mHealth apps. Despite this, no review has comprehensively summarized the findings from studies on this subject matter.

Objective: This systematic review aimed to investigate patients' perspectives and awareness of the confidentiality, privacy, and security of the data collected through mHealth apps.

Methods: Utilizing the PRISMA guideline, a comprehensive literature search was performed in three electronic databases: PubMed, Ovid, and ScienceDirect. All the retrieved articles were screened according to specific inclusion criteria to select relevant articles published between 2014 and 2022.

Results: A total of 33 articles exploring mHealth patients' perspectives and awareness of data privacy, security, and confidentiality issues and the associated factors were included in the systematic review. Thematic analyses of the retrieved data led to the synthesis of four themes: concerns about data privacy, confidentiality and security (2) awareness, (3) facilitators and enablers, and (4) associated factors. Patients demonstrated discordant and concordant perspectives regarding data privacy, security and confidentiality, as well as approaches to improve the use of mHealth apps (facilitators) such as protection of personal data, ensuring health status or medical condition are not mentioned, brief training or education on data security, and assuring data confidentiality and privacy. Likewise, awareness of the subject matter differed across studies, suggesting the need to improve patients' awareness of data security and privacy. Patients' concerns on the subject matter were influenced by sociodemographic characteristics such as age, income level, marital status, experience with mHealth apps, satisfaction levels, data type and data stage.

Conclusions: Patients expressed diverse views on mHealth apps' privacy, security and confidentiality, with some issues raised affecting the technology utilisation. The present findings may assist mHealth app developers and other stakeholders in improving patients' awareness and adjusting current privacy and security features in mHealth apps to enhance their adoption and utilisation.

(JMIR Preprints 10/07/2023:50715)

DOI: <https://doi.org/10.2196/preprints.50715>

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 visible to the public.

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <http://www.jmir.org/>, I will be able to make my manuscript PDF available to the public.



Original Manuscript

Original Paper

N. Alhammad, M. Alajlani, A. Abd-alrazaq, G. Epiphaniou and T.N. Arvanitis

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

A systematic review of patients' perspectives on data confidentiality, privacy, and security of mobile health applications

Abstract

Background: Mobile Health Applications (mHealth apps) have the potential to enhance healthcare service delivery. However, concerns regarding patients' confidentiality, privacy, and security consistently affect the adoption of mHealth apps. Despite this, no review has comprehensively summarized the findings from studies on this subject matter.

Objective: This systematic review aimed to investigate patients' perspectives and awareness of the confidentiality, privacy, and security of the data collected through mHealth apps.

Methods: Utilizing the PRISMA guideline, a comprehensive literature search was performed in three electronic databases: PubMed, Ovid, and ScienceDirect. All the retrieved articles were screened according to specific inclusion criteria to select relevant articles published between 2014 and 2022.

Results: A total of 33 articles exploring mHealth patients' perspectives and awareness of data privacy, security, and confidentiality issues and the associated factors were included in the systematic review. Thematic analyses of the retrieved data led to the synthesis of four themes: concerns about data privacy, confidentiality and security (2) awareness, (3) facilitators and enablers, and (4) associated factors. Patients demonstrated discordant and concordant perspectives regarding data privacy, security and confidentiality, as well as approaches to improve the use of mHealth apps (facilitators) such as protection of personal data, ensuring health status or medical condition are not mentioned, brief training or education on data security, and assuring data confidentiality and privacy. Likewise, awareness of the subject matter differed across studies, suggesting the need to improve patients' awareness of data security and privacy. Older patients, history of experiencing data breaches, and those belonging to the higher income class were more likely to raise concerns about data security and privacy of mHealth apps. These concerns were not frequent among patients with higher satisfaction levels and those perceiving the data type to be less sensitive.

Conclusion: Patients expressed diverse views on mHealth apps' privacy, security and confidentiality, with some issues raised affecting the technology utilisation. The present findings may assist mHealth app developers and other stakeholders in improving patients' awareness and adjusting current privacy and security features in mHealth apps to enhance their adoption and utilisation.

Keywords: mHealth apps, mobile health, privacy, confidentiality, security, awareness, perspectives

Introduction

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 (HC) industry and research field [2]. The coronavirus disease 2019 pandemic has further accelerated reliance on digital health [3]. The mHealth apps are used by patients 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]. Besides, mHealth apps provide easy access to HCPs by connecting them to clinical information systems (CISs) resources like electronic health records (EHRs) [6]. Although mHealth apps could provide evidence-based and cost-effective health data and two-way communications with patients and their HCPs in a remote setting, a few barriers blocked the expansion of mHealth apps in the HC industry. Data confidentiality, privacy, security, and regulatory supervision of the apps are some known barriers that hinder mHealth adoption in the HC field.

Despite various benefits of mHealth apps, data confidentiality, privacy, and security issues caused patients or the public to display less interest and low confidence in mHealth app practice [7]. It could be due to the uncertainty about the information gathered or kept in mHealth apps, the function of the stored data, and who can view or access the data [4]. The term 'confidentiality' is defined to be 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]. Bhuyan et al. [9] study mentioned that the National Committee on Vital and Health Statistics (NCVHS) defined privacy as 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. Whereas security is defined as the physical, mechanical, or legislative mechanism or tools to shield personal health information from unauthorised disclosure [10].

Confidentiality, privacy, and security act as challenges in boosting mHealth app adoption. Patients' perception of these issues may influence their adoption of mHealth apps but such events are context-dependent. While users are more likely to raise concerns about privacy or confidential issues when probed about mHealth apps, such perceptions may not ultimately influence their behaviour towards actual usage or adoption of such apps. Thus, it is pertinent to explore whether privacy concerns are prioritised by users when they engage in mHealth apps and if such concerns affect their decision to use the apps or not.

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 [9]. In addition, data management and storage, data privacy disclosure, data integration, data encryption, app operability, and authentication are established factors contributing to data breaches [9].

Several studies have highlighted the connection between patients' awareness and the risk of data breaches. End-users have an obligation for the security and privacy of their data, to be maintained [4]. 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. Healthcare app developers must protect sensitive patient data by complying with data privacy regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). To ensure data privacy and security, mHealth apps are encouraged to incorporate data encryption, implement secure authentications, and perform regular risk assessments [10]. While HIPAA encompasses physical, administrative and technical aspects to ensure the security of personal health information, GDPR requires health centres or organisations to collect detailed consent from users before recording their personal data, and giving them the right to access, amend, delete or restrict processing their data. These privacy requirements for app security are not only known by mHealth app providers but among patients and users as well [10,11]. This represents another dimension that may influence patients' perspectives and adoption of mHealth apps.

Despite the pivotal role of patients' views and awareness in the successful implementation of mHealth apps, as demonstrated in several studies, the findings are yet to be summarised to elucidate the barriers and facilitators, which may assist clinicians, healthcare professionals, policymakers and other stakeholders in their decision-making process. A previous systematic review on the security and privacy of mHealth apps was conducted almost a decade ago and did not focus on any specific stakeholder [12]. Meanwhile, two other reviews relating to the research topic entailed a narrative and scoping review [13,14], which is open to bias since the methods used in retrieving the reviewed articles were not succinctly described. This study aims to fill the research gap by conducting a systematic review to elucidate patients' perspectives and awareness of privacy, security and confidentiality of mHealth apps, as well as the associated factors.

Methods

This study was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [15]. The systematic review has been registered with PROSPERO with the registration number: CRD42023456658.

Search Strategy

The systematic article search was conducted using three electronic databases: PubMed, PsycNet and ScienceDirect. PsycNet was assessed via Ovid, as a search interface. These databases were selected given their suitability and specificity for research in health and medical sciences, thus increasing the chances of retrieving articles relevant to the research topic. The first author of this systematic review performed the literature search from February 2022 to April 2022. Articles published between 2014 and 2022 and written in English were considered for the literature search. We focused on studies published from 2014 to 2022, given the growing interest in the usage of mHealth apps in the last decade [2].

Aligning with the objectives of this review, the search items were broadly categorised into three components or groups of keywords. Alternative keywords were permitted for each component as denoted by the Boolean operator "OR". The separator "AND" was then used in combining each component with other wordings. The search query for each of the databases is presented

in Table 1. Detailed information on the search query can be gleaned from the supplementary material.

Table 1: The search terms used and the total number of publications retrieved from each database

Database	Search string and search terms		Initial search results (No. of articles)	Date of acquisition
Scopus	Main searching terms-using document title, abstract	("Mobile health" OR mhealth OR "mobile phone*" OR "Smart phone*" OR Smartphone* OR tablet*) AND ("Perspective OR opinion* OR attitude* OR perception* OR awareness) AND (Privacy OR confidential* OR security).	1277	20/02/2023
Science Direct		("Mobile health" OR mhealth OR "mobile phone") AND ("Perspective OR opinion OR awareness) AND (Privacy OR confidential OR security)	7156	21/03/2023
APA PsycNet		"Mobile health" OR mhealth OR "mobile phone*" OR "Smart phone*" OR Smartphone* OR tablet* AND "Perspective OR opinion* OR attitude* OR perception* OR awareness AND Privacy OR confidential* OR security	441	19/04/2023

Study eligibility criteria

The inclusion and exclusion considerations of the research are presented in Table 2. The first inclusion criterion was the document type in which only published original articles were considered. Other document types, such as review articles, chapters in books, books, and conference proceedings were all excluded. The next inclusion criterion was the study duration, whereby only the articles published from 2014 to 2022 were selected. The inclusion or exclusion of retrieved articles was based on the agreement between the authors. Issues arising during the process were resolved by consensus.

Table 2. The inclusion and exclusion criteria

Consideration factors	Inclusion criteria	Exclusion criteria
Study design	Empirical studies involving qualitative, quantitative methods, and/or mixed-	Reviews (systematic, scoping, narrative, rapid, and meta-analysis)

	methods	
Publication type	Peer-reviewed journal articles	Editorial letters, protocols, expert opinions, policy briefs, thesis/ dissertation, conference papers
mHealth apps	Studies involving mHealth apps regardless of their aim, target disease, and system type (IOS, Android etc.)	Studies involving apps that are not linked to CISOs
Study participants	Studies involving patients with or without HCPs like physicians, nurses, pharmacists, and care teams regardless of demographic characteristics (i.e., age, gender, ethnicity etc.)	Studies solely involving app developers, HCPs, and telehealth providers
Outcomes	Experience, perceptions, awareness, and knowledge of patients after practical use of mHealth apps	The description of the impact of mHealth apps and the patient-HCP relationship
Language	English	Other languages
Year	2014 onwards	Before 2014

Study selection

Two researchers performed the study selection process independently. Articles retrieved from the primary literature search from each database were sent to the researcher's email repository and stored for future reference. The screening process was carried out using the filter feature available in all three databases. The initial search results were checked for duplicates, which were then identified and removed accordingly. The last screening stage was the full-text reading. The inclusion or exclusion of retrieved articles was based on the agreement between the authors. Issues arising during the process were resolved by consensus.

Data Extraction

The final articles included in this study were assessed, reviewed, and examined upon completing the eligibility process. An Excel spreadsheet form was created to use in data extraction. The data extracted from the studies were as follows: first author, year of publication, study location, study design, types and purposes of mHealth apps, issues relating to privacy, security and confidentiality of mHealth apps, and the main findings. The data extraction was performed by the first author; thus the intercoder agreement was not assessed.

Quality Appraisal

Quality appraisal was not performed in the review due to the heterogeneity of the research

objectives, designs and methodology used in the included studies [16].

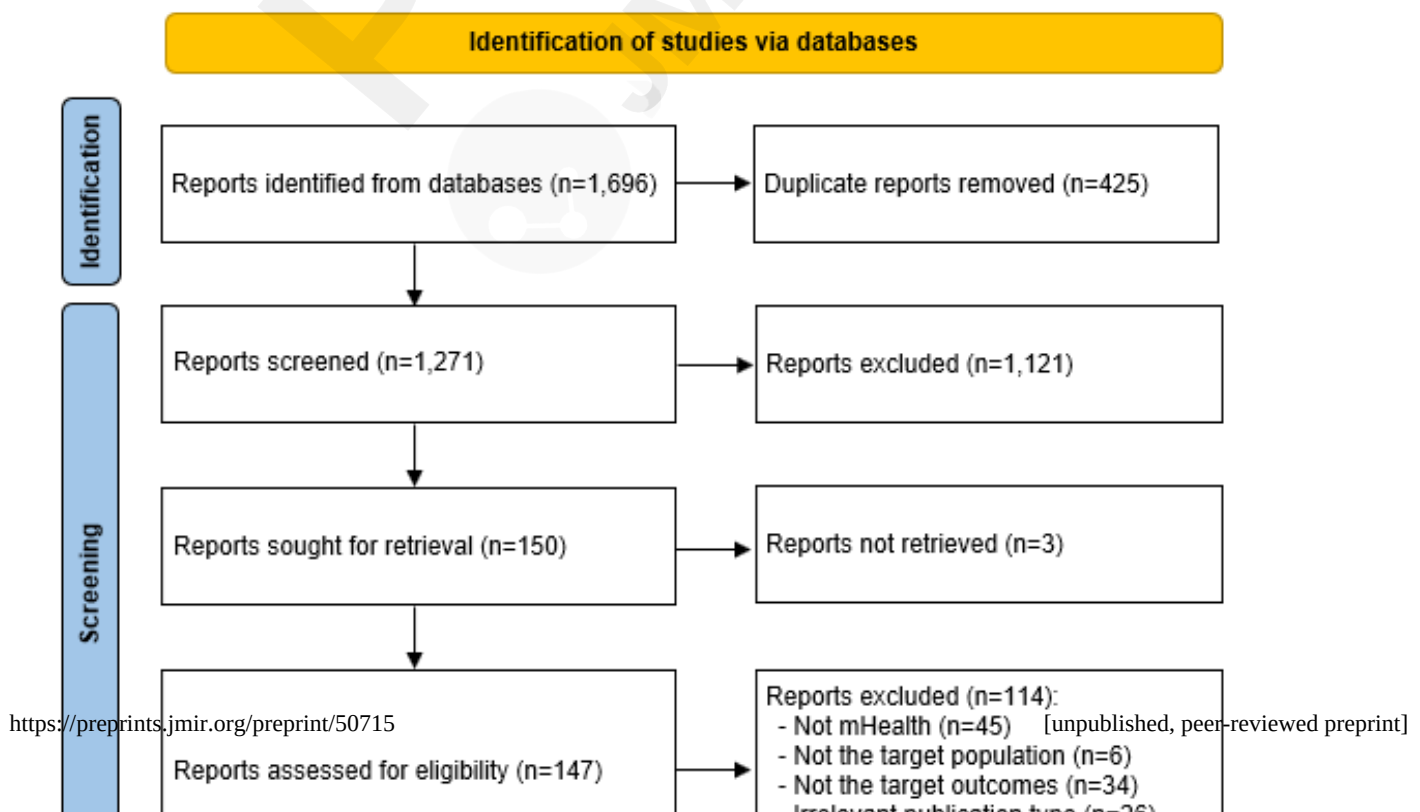
Data Synthesis

A narrative synthesis was considered in this paper due to the heterogeneity of the study designs used in the articles. Specifically, thematic analysis was performed to summarise the findings of the included studies. The data extracted were converted into useful data and directed by distinguishing the concepts and themes that link and connect all the obtainable data from the papers included. All the authors participated in the discussion to determine the themes that will be synthesised from the analysis. The themes decided were: (1) Barriers and facilitators of using mHealth apps (2) Recommendations to increase the use of mHealth apps by addressing privacy, security and confidentiality issues. Any further analysis and re-assessment of the themes and sub-themes were performed continuously.

Results

Search outcomes

A total of 1696 articles were retrieved from the initial search: PubMed (n = 659), Science Direct (n = 172) and OVID (n = 865). Of the search results, 425 were removed from the list as duplicates (Figure 1), while 1,121 were considered ineligible upon screening the titles and abstracts. The 150 remaining articles were then subjected to a full-text review, which led to the final selection of 33 articles for the systematic review based on the inclusion and exclusion criteria (Figure 1).



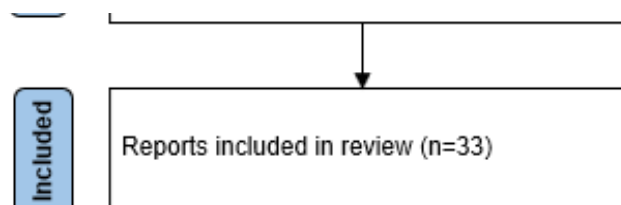


Figure 1: PRISMA flow diagram of the study selection process. In terms of study location, most of the studies were conducted in high-income and developed countries (n = 26) compared to those undertaken in middle and low-income countries (n = 7). While 3 articles emphasised the general usage of mHealth apps for routine health records, 12 articles focused on specific mHealth apps for collecting patients' health data and management of various medical conditions such as chronic obstructive pulmonary disease [17], cancer [18-21], diabetes [22], and pregnancy care [23,24] (Table 4).

Table 3: Descriptive information of the articles

Variables	Frequency	%
Year of publication		
2014	2	6
2015	2	6
2016	2	6
2017	2	6
2018	4	12
2019	7	21
2020	4	12
2021	9	27
2022	1	3
Study designs		
Qualitative	13	39
Quantitative	11	33
Mixed method	9	27
Study locations		
High income	26	78
Middle-high income	7	22
Low income	0	0
Purpose of mHealth apps		
Routine electronic health records	3	9
Specific apps for patient management	12	36
Unspecific	18	55



Table 4. Details of author name, publication year, type of intervention, study design, setting, instruments and findings from the 33 reviewed articles

Authors (Year)	Type of intervention	Study design	Study location	Data collection method/s	Main findings	Themes identified
Wyatt et al. [25]	PhotoExam Apps [Electronic health records (EHRs)]	Quantitative	United States	App usage & survey	Only 3% (2/71) of patients expressed privacy or confidentiality concerns related to the photos taken, b) 26% (18/70) of patients mentioned that security features of the apps were explained by the HCPs, c) 16% (11/70) indicated that security features were not explained, and the majority (41/70, 59%) of them did not remember/unsure if security features were explained	Concerns about privacy Concerns about confidentiality
Zhou et al. [4]	mHealth apps	Mixed-methods	USA	Questionnaire and qualitative analysis (semi-structured interview & psychometric analysis)	a) From the 1 st category of the questionnaire, participants had some level of concern about the privacy of their personal data and wanted to have some specific protections b) From the 2 nd category of the questionnaire, participants believed that a level of privacy protection is currently available in mHealth apps.	Concerns about data privacy Concerns about data security

					c) From the 3rd category of the questionnaire, participants desired to have informed consent, access control, privacy policy, and remote wipe features in mHealth apps. d) Two-thirds of the users (66.7%) stated that the cost of apps and lack of security features in mHealth apps were the main barriers to adopting the technology.	
Natsiavas et al. [26]	eHealth data	Quantitative	14 European countries	Questionnaire	a) 11.96% did not think about possible health data risks, and 36.41% felt informed about these risks. b) 66.21% of the responders did not read “Terms and Conditions”, with more than 30% declaring that they did not feel it was worthy and given the time required to read them and 19.79% declaring indifference towards them. c) 26.09% of the responders felt confident regarding their eHealth data privacy, 38.04% felt concerned but helpless, and 16.3% stated that they avoid using eHealth services	Awareness of data privacy and confidentiality Concerns about data privacy

					due to the lack of confidence regarding their data handling. d) 20% of the responders felt their privacy was fully covered in the “Terms and Conditions” of the apps, and 12.50% declared that they did not understand them. e) 72.46% of respondents were willing to share their personal data for research purposes, at least under the terms of anonymisation.	
Alaiad et al. [27]	mHealth model	Quantitative	Jordan	Questionnaire	a) Security and privacy risks have a direct negative effect on the patient’s intention to use mHealth b) mHealth patients in developing countries are often using M-Health services at their own risk, which makes them prone to data breaches and misuse by unknown parties	Data security Data privacy
Özkan et al. [28]	Electronic health records (EHRs)	Quantitative	Turkey	Survey	a) Majority of the participants (60.9%) stated that they did not know who had the right to access their medical records, and 7.4% believed to have comprehensive knowledge on the topic. b) The medical reports of 9.7% of the respondents had	Awareness of data confidentiality and privacy Data Confidentiality Data privacy

					been used/released without their consent. c) 15.1% stated that they avoided being tested due to violation risks, and 3.5% asked their doctors to enter a less embarrassing health status in their records. d) Most participants (94%) responded that they should have full access to their medical data, while 50% of respondents want other parties (children, parents, doctors, spouses, and other doctors/hospital staff) to have limited access rights.	
Glauser et al. [29]	NeuroPath (mHealth apps)	Qualitative	USA	App usage & telephone interview	14 (63.6%) respondents stated that they wait before trying new technology and 6 (27.3%) of these respondents were concerned about data security when asked about their readiness to adopt new technologies.	Concerns about data security
Zhou et al. [30]	SecSim (Security Simulator)	Mixed-methods, quasi-experimental and interview session	USA	Apps usage, IBM Post-Study System Usability Questionnaire (PSSUQ) & open-ended	a) The comparison between the pre-and post-security education selection in security settings indicated that 21% (14/66) to 32% (21/66) participants chose a stronger security measure in	Concerns about data security

				interview questions	text encryption, access control, and image encryption; 0% (0/66) to 2% (1/66) participants chose a weaker measure in these 3 security features; and the remainder kept their original selections b) A significant percentage of patients (21%-32%) need guidance to make an informed selection in security settings	
Barutçu et al. [31]	e-Pulse (mHealth apps)	Quantitative	Turkey	Survey	a) Participants considered mHealth apps as less credible in protecting their personal information. b) Positive relationships between user satisfaction level from mHealth apps and ease of use, trust, privacy, usefulness and information quality of mHealth apps. c) mHealth apps' user satisfaction was negatively influenced by the privacy of mHealth apps. d) Perceived ease of use, trust, privacy, perceived usefulness and information quality were the major factors influencing satisfaction and	Concerns about data privacy Associated factors: satisfaction with mHealth apps

					intention to adopt mHealth apps.	
Bauer et al. [32]	Mobile health platform supporting Collaborative Care	Mixed-methods	USA	Apps usage, surveys & interviews	a) Patients felt the data they submitted was not entirely secure, but they did not believe that the information reported in the apps was highly personal, therefore the potential for a data breach was not a major concern. b) Some patients wished to have a better understanding of who else had access to their health information, and the ability to control such access. (Based on qualitative findings)	Data security Awareness of data security and privacy
Goetz et al. [33]	PRELAX (eHealth apps)	Mixed-methods	Germany	Apps usage, self-administered questionnaire & semi-structured interviews	a) Hospitalized women (6/30; 20%) were worried about unauthorized third-party access to their stored medical data. b) Several women (8/30; 27%) expressed concerns about data security, especially in the field of mobile apps, since many free apps make private data easily accessible c) Data security and personal data storage in pregnancy applications were general	Data confidentiality Data privacy

					causes for concern	
Richardson and Ancker [34]	Electronic health record (EHR)	Quantitative	USA	Survey	a) About three-quarters of individuals believed that storing medical information on the phone would threaten privacy and security (74% in 2013, 75% in 2014). b) About two-thirds thought that sharing data between a mobile device and a doctor's EHR would threaten privacy and security (69% in 2013, 67% in 2014) c) Participants expressed concern about worsened privacy and security with storing data on mobile phones and mobile phone-EHR communication (74% and 69% respectively) than with EHRs and physician health information exchange (41% and 47%).	Data privacy Data security
Sanger et al. [35]	Post-acute care apps	Qualitative	USA	Semi-structured interviews	Participants were most concerned about the collection and transmission of particularly sensitive information such as photos of the groin area	Data privacy Data security
Dang et al. [36]	Not specific	Quantitative survey	China	Survey	Privacy concern among patients was positively enhanced by perceived health	Data privacy Data security

					information sensitivity (beta path coefficient 0.505, $P<0.001$). Patients' health information disclosure intention decreased significantly with higher concern levels (beta path coefficient -0.338, $P<.001$). The relationship between perceived health information sensitivity and privacy concerns was negatively moderated (beta path coefficient -0.171, $P = 0.092$) by the informational support dimension. A similar moderating effect was demonstrated in the association between privacy concerns and health information disclosure intention (beta path coefficient -0.105, $P = 0.092$).	Associated factors: Health information disclosure
Alwashmi et al. [17]	Not specific	Mixed-method	Canada	In-depth interviews and survey instrument	The barriers to adoption were technical issues, lack of awareness, potentially limited uptake from older adults, privacy, and confidentiality issues.	Awareness of data privacy and confidentiality Associated factors: Demographic factors Data privacy issues and confidentiality issues

						Facilitators and Enablers
Biswas et al. [37]	ACCU3RATE (a specific AI-enabled mhealth app rating)	Quantitative	Multinational study	Survey instrument	Patients presented positive feedback regarding the apps' features for accessibility, protection and privacy of patients data	Data privacy
Casilang et al. [38]	Mobile health for the development of an exclusive breastfeeding tool	Qualitative	Dominican Republic	Focus-group discussion	Barriers to mHealth use included the cost of internet service, privacy concerns, and perceived credibility of information sources	Facilitators and Enablers Data Privacy
Zhang et al. [39]	Unspecific	Quantitative	USA	Web-based Survey	Data type ($P = 0.003$), data stage ($P < 0.001$), privacy victimization experience ($P = 0.01$), and privacy awareness ($P = 0.08$) demonstrated positive effects on patients' privacy concerns. Higher privacy concerns were reported for social interaction data ($P = 0.007$) and self-reported data ($P = 0.001$) than for biometrics data. Privacy concerns were also higher for data transmission ($P = 0.01$) and data sharing ($P < 0.001$) than for data collection. Privacy concerns affected the attitude toward privacy protection ($P = 0.001$), thereby affecting continuous usage intention.	Privacy concerns Associated factors: data type and stage, victimisation experience

Harris et al. [40]	Mobile phone health apps	Mixed-method	Pakistan, Tanzania , Kenya, Nigeria, Bangladesh	Scoping study and analysis of survey data	Stakeholder willingness was high, provided challenges are addressed in technology, infrastructure, data security, confidentiality, acceptability, and health system integration. Mobile consulting can reduce affordability barriers and facilitate care-seeking practices.	Data security Data confidentiality
Moodley et al. [18]	Mobile phone health apps	Mixed-method	South Africa	Survey and focus-group discussion	Users were interested in the use of mobile phone apps for health intervention in receiving Pap smear results and appointment reminders. However, concerns were relayed regarding the confidentiality of SMS messages, loss/theft of mobile phones, receiving negative results, and accessibility/clarity of the language used to convey messages	Data confidentiality
Li et al. [24]	mHealth technology for monitoring pregnancy care	Qualitative	Australia	In-depth interviews	The clinical and technical challenges in the introduction of mHealth for pregnancy care were also identified. whereas usability and data privacy were among the main concerns of the participants	Data privacy Facilitators and Enablers
Gill et al.	mHealth	Mixed-method	USA	Survey, semi-	Qualitative analysis revealed	Data security

[21]	technology to support postabortion			structured interviews	that participants preferred a comprehensive website with secured email or text notifications to provide tools and resources for emotional well-being, contraceptive decision-making, general sexual health, and postprocedural care.	Facilitators and Enablers
Bradbury et al. [19]	Remote real-time videoconferencing for cancer patients	Quantitative and experimental	USA	Pretest, post-test data counselling	Most patients reported that their privacy was respected—post-V1: 56/57 (98%); post-V2: 40/41 (98%). Meanwhile, some patients reported concerns that RVC might increase the risk of a confidentiality breach of their health information—post-V1: 14/57 (25%); post-V2: 12/41 (29%).	Data Confidentiality
Al-Anezi et al. [41]	Unspecific	Quantitative	Saudi Arabia	Survey	Fear of privacy violations, fear of loss of personal data and information, and lack of technical support were highlighted as the main reasons for the lack of motivation to adopt the mhealth system	Privacy issues
Ermakova et al. [42]	Health clouds	Quantitative	Germany	Survey	Confidentiality assurance was vital in influencing individuals' acceptance of health clouds for sensitive	Data confidentiality

					medical data, but such an effect was lacking for non-sensitive medical data.	
Rodrigues et al. [43]	Unspecific	Qualitative	South India	In-depth interviews	Participants perceived the risk of unintentional disclosure of their HIV status and the stigma thereof via the intervention and took initiatives to mitigate this risk	Data confidentiality
De Vries et al. [22]	Unspecific	Qualitative	Netherlands	Focus-group discussions and interviews	The use of mobile apps for reporting adverse drug reactions and obtaining safety guidelines included the source of safety information provided through the apps, security of the apps, type of feedback presented on reported ADRs, storage pattern of ADR reports and the type of drug news, ease of use, type of language	Data security Facilitators and enablers
Al-Mahrouqi et al. [44]	Unspecific	Qualitative	Oman	Semi-structured qualitative interviews	Although clients acknowledged the positive impact of telehealth in improving mental healthcare services in Oman, Primary concerns were related to privacy, concerns toward the security of telehealth systems, lack of public telemental health services, lack of specified telemental health	Concerns about data privacy Concerns about data security

					guidelines, shortage of trained therapists, limited access to high-speed Internet, electronic devices	
Turcotte et al. [45]	Teleconsultation (Asy your Pharmacy; ASP)	Qualitative	Canada	Semi-structured interviews	Although both users and non-users presented positive experiences and perspectives of the AYP platform are mostly positive, concerns were raised regarding patients' safety.	Data security issues
Hackett et al. [23]	Mobile phone apps	Qualitative	Tanzania	Semi-structured interviews	a) Perceptions of personal privacy and confidentiality were negatively and positively impacted by the use of new technologies to capture health service user data during pregnancy and childbirth. b) Women's concerns regarding privacy aligned closely with a belief that pregnancies and expected delivery dates must be kept secret, reflecting fears that pregnancy renders women vulnerable to witchcraft by jealous neighbours. c) They were also concerned that health workers' male partners could access their private information	Concerns about data privacy Concerns about data confidentiality Facilitators and Enablers

Morton et al. [46]	Mobile phone apps	Mixed-method	Many countries	Survey and in-depth interviews	Concerns regarding data security were prevalent. Data security, content quality/accuracy, ease of use, and cost were among the prioritized mHealth features. The ability to share data with others was described as vital by fewer than half of the respondents	Concerns about data security
Cavazos-Rehg et al. [47]	mHealth mental intervention	Quantitative	USA	Survey	The main reasons presented for unwillingness to obtain parental consent to participate in the intervention included the importance of retaining privacy and the feeling that parents lack awareness or understanding of mental health issues	Privacy concerns Awareness of data privacy
Sangers et al. [20]	mHealth apps for skincare screening	Qualitative	Netherlands	Semi-structured interviews	The main barriers to using mHealth apps included privacy concerns, perceived lack of value, perception of untrustworthiness, preference for a doctor, a complex user interface, and high costs.	Privacy concerns Facilitators and Enablers
Hattingh et al. [48]	mHealth in pharmacy settings	Qualitative	Australia	In-depth interviews and focus group discussion	Consumers indicated a desire to receive information in a way that respects their privacy and confidentiality, in an appropriate space. Important areas were	Privacy, security, and confidentiality issues

					identified that require improved protection of privacy and confidentiality during pharmacy interactions	
--	--	--	--	--	---	--

mHealth apps for specific intervention

A total of 12 studies included in this review reported the use of mHealth apps for patient health data collection and management of specific health conditions. Three studies entailed the use of specific mHealth apps for assessing patient treatment progress [25, 29, 35]. PhotoExam Apps [25] entailed the collection of patients' photos, which are then assessed for patient response to the treatment provided. Glauser et al. [29] developed an application named "Neuropath" with the support of Apple, Institutional Department of Neurosurgery and the Department of Information Technology. The areas targeted by the app include patient surgical preparation, prevention of perioperative risk, wound care, activity monitoring, and opioid use management. Meanwhile, Sanger et al. [35] focused on mHealth apps for post-acute care.

Regarding specific medical conditions, three studies focused on mHealth apps for pregnancy management, such as patient engagement pregnancy application (PRELAX) [33], pregnancy care [24], and support for post-abortion [14]. Other studies entailed mHealth apps for real-time videoconferencing for cancer patients [19], mental health intervention [47], support for collaborative care [32] and teleconsultation for pharmaceutical services [43].

Lastly, two studies emphasised the security of mHealth apps without focusing on medical conditions or groups of patients. Zhou et al. [30] developed a security simulator named SecSim to reveal the consequences of selecting different security options available in the security settings of mHealth apps. Meanwhile, Biswas et al. [37] used a specific AI-enabled mHealth app rating, ACCU3RATE, to obtain users' feedback on the security features. The influence of these interventions on patient perception of the security, confidentiality and privacy of data collected via mHealth apps are presented in the thematic analysis.

Results from Thematic Analysis

The thematic analysis generated 4 broad themes from the findings of the studies: (1) Privacy, confidentiality and security, (2) Awareness of privacy, security, and confidentiality, (3) Facilitators and enablers, and (4) Associated factors. The following subsections present more detailed information about the synthesised themes.

Theme 1: Privacy, confidentiality and security

As expected, all the included studies investigated privacy, confidentiality, and security issues relating to patients' usage of mHealth. Different levels of privacy and confidentiality concerns were reflected in the studies. In five studies, less than half of the patients expressed concerns about the privacy or confidentiality of the various data required in mHealth apps [19, 25, 26, 28, 33]. Meanwhile, in two studies, more than 50% of the respondents raised diverse issues regarding the privacy and confidentiality of their data [4, 34]. In terms of data security, three studies that employed quantitative design revealed a higher proportion of patients (>50%) acknowledging issues relating to data security (29, 30, 34).

This theme was also depicted in several qualitative and mixed-method studies [4, 20, 22 - 24, 39, 37, 40, 45, 48]. For instance, patients opined that the privacy protection level in

mHealth apps needs to be improved (4, 29; 38). Meanwhile, patients felt their data were not completely secure and were concerned about data breaches [21, 32]. In three studies, issues relating to privacy, confidentiality and security were identified as barriers to mHealth use [24, 38, 40]. Meanwhile, Biswas et al. [37] found that respondents were satisfied with the apps' features for the protection and privacy of patients' data.

Theme 2: Awareness of privacy, security, and confidentiality

Patients' awareness of mHealth apps' privacy, security and confidentiality was highlighted in four studies [4, 25, 26, 28]. Nevertheless, the awareness level differed across studies.

Natsiavas et al.[26] found that 12% of patients in their study were unaware of the possibility of health data risks, whereas a higher percentage of participants (61%) in the study by Özkan et al. [28] did not know who had the right to access their medical records. Thematic analysis of the data gathered by Bauer et al. [32] revealed that patients opted for a better understanding of other parties who have access to their health information, and their capacity to regulate such access. Meanwhile, Alwashmi et al. [17] and Zhang et al. [39] identified awareness of privacy and confidentiality issues as barriers to adopting mHealth apps and raising concerns about data privacy, respectively.

Theme 3: Facilitators and Enablers

The third theme synthesised in this SLR is the facilitators for increased usage or adoption of mHealth apps among patients based on their perceived benefits of mHealth apps and recommendations to address data privacy, security and confidentiality issues. Six studies reported the perceived benefits of mHealth apps that may reduce patients' concerns about issues relating to data privacy and security, thus improving the adoption rate of such apps [17, 21 – 24, 30]. Some of the benefits highlighted by patients include improved health status by reducing the rate of hospitalisation [17], increased trust, better patient-healthcare professional relationships [22, 23], and exchange of information in real time [21]. Overall, patients viewed mHealth apps installed on smartphones as an added value, which assisted in improving their confidentiality, trust, and relationship with healthcare personnel.

As for recommendations and facilitating conditions to address data privacy, security and confidentiality issues relating to mHealth, the consistent points raised in the studies were the protection of personal data, ensuring health status or medical condition is not mentioned, brief training or education on data security, and assuring data confidentiality and privacy [21, 24, 30]. Gill et al. [21] found that participants prioritised privacy and confidentiality by preferring discrete mHealth designs without mentioning the specific medical condition that prompted them to visit the clinic.

Theme 4: Associated factors

The last theme gleaned from this review was the factors associated with patients' concerns regarding issues relating to data confidentiality, privacy and security when using mHealth apps. This theme was synthesised from the findings reported in five studies [4, 31, 36, 39, 42], which comprised patients' socio-demographic factors, satisfaction with mHealth, data type and stage, and experience with mHealth apps.

In terms of socio-demographic factors, Zhou et al. [4] found that married patients demonstrated higher information security and privacy concerns and desired more

stringent security protection compared to single patients. The weakest concerns about privacy and security were exhibited by users with less than 10,000 USD in annual income compared to the patients earning more than 75,000 USD annually income. Likewise, patients in the older age group (51-65 years old) reflected a higher level of concern about privacy in mHealth apps relative to the younger age group (18-28 years old). In terms of experience, participants who had previously used mHealth apps had greater concerns for data security and privacy despite still being interested to continue using the technology.

Only one study reported the association between satisfaction levels with mHealth apps and privacy concerns [31]. Specifically, a positive relationship was observed between user satisfaction levels from mHealth apps and privacy concerns. Meanwhile, Dang et al. [36] found that a higher perceived health information sensitivity heightened the privacy concerns (beta path coefficient = 0.505, $P < 0.001$) raised by patients regarding mHealth apps. The provision of informational support moderated the association between privacy concerns and health information sensitivity.

Zhang et al. [39] revealed the diverse levels of privacy concerns depending on data type, data stage, and privacy victimization experience. For instance, privacy concerns were higher for patients' social interaction, self-reported, and biometrics data. Users were less concerned about privacy issues during data collection compared to data transmission and sharing stages. These events had negative impacts on the continuous intention to use mHealth apps [39]. Ermakova et al. [42] also found that patients' acceptance of health clouds for non-sensitive medical data was not significantly affected by confidentiality assurance; however, the relationship was significant for sensitive medical data.

Discussion

This systematic review evaluated patients' perspectives and understanding of data confidentiality, privacy, and security of mHealth apps connected to CISs. A total of 33 relevant articles were extracted and included in this systematic review upon employing the PRISMA guidelines. Descriptive analyses depict that most of the studies were conducted in developed or high-income countries ($n = 26$) compared to those undertaken in developing, underdeveloped or middle to low-income countries ($n = 7$). These findings reflect the disparity in the implementation and adoption of mHealth apps in line with different countries' economic status and infrastructural capacity. This is evident in the use of mHealth apps for the management of specific medical conditions in the United States, the United Kingdom, Australia, and Turkey, whereas the few studies conducted in less developed countries focused mainly on either the feasibility or introductory stages of general mHealth apps. Notwithstanding the patients' socio-economic status, data privacy, confidentiality, and security issues were highlighted in most studies.

The extensive investigation of mHealth apps was also reflected in the diverse medical conditions in which the technology has been explored, such as chronic obstructive pulmonary disease [17], cancer [19, 20], postabortion care [21], diabetes [22], and pregnancy care [24]. Descriptive analyses also revealed the use of various research methods (qualitative, quantitative and mixed methods) in the reviewed articles, which is not surprising given that the research topic can be explored via interviews, focus-group discussions and surveys.

Thematic analyses of the qualitative studies revealed four main themes, comprising primary concerns on privacy, confidentiality and security of data, awareness of privacy,

security, and confidentiality issues, facilitators and enablers, and associated factors. Regarding the first theme, patients were concerned about data security and security, particularly in terms of the collection and transmission of sensitive information such as identity-revealing data and images of body parts [22, 33, 35]. Some hospitalised patients were even more concerned about unauthorised third-party access to their medical data given that mHealth apps are mostly free and easily accessible [17, 33]. In contrast, some patients were indifferent to these issues in the same studies as they were willing to use mHealth apps and share their health data with healthcare professionals. These diverse views could be linked to patients' consideration of the benefits and risks associated with using mHealth apps for routine health records or managing their health conditions.

We observed concordant perspectives of the research topic as patients and end users consistently raised concerns about data privacy, security and confidentiality issues that prevented them from using mHealth apps [18, 20, 35]. This result aligns with a previous review by Nurgalieva et al. [13] in which low levels of security and privacy were reported as the main reason for low usage among patients and end users. Serious issues may arise from mobile health applications with low levels of security or privacy, and such events may have severe consequences for users and organisations.

Given the extensive privacy and security issues raised in the reviewed studies, the findings suggest the need for mobile health environments to improve the security of these apps by exploring advances in cyberspace security [4]. Likewise, both reviews by Martínez-Pérez et al. [14] and Nurgalieva et al. [14] highlighted security incidents, including vulnerabilities discovered in widely used mobile health apps and malware attacks. The concerns raised by patients are plausible since the proliferation of mobile devices with location sensors has facilitated easy access to location-based services [14]. These advanced devices transmit the user's location information to third-party location servers, which are accessible by other service providers. Users aware of this potential data breach may feel they are continuously tracked. In the present review, some patients seem to be aware of the risk of third-party and unauthorised access to their medical data [4, 25].

For the second theme, both qualitative and empirical findings reflected that patients' awareness of privacy and security of mHealth apps differed across studies. For example, more than two-thirds of participants expressed their concerns about personal data security and privacy and requested user authentication and data encryption to protect user data [4, 34] and less than 12% were unaware of the risk of health data breaches [19, 31]. Meanwhile, more than half of the respondents in the studies conducted by Özkan et al. [28] and Wyatt et al. [25] were unsure about the privacy and security information on their mHealth apps. Thus, the different awareness level among patients may influence their diverse perspectives on the privacy and security of mHealth apps.

The third theme emerging from the thematic analyses entailed the facilitators for increased usage or adoption of mHealth apps based on patients' perceived benefits of mHealth apps and suggestions to address data privacy, security and confidentiality issues. Resultantly, improved health status [17], better patient-healthcare professional relationships [22, 23], and trust were the main benefits mentioned by patients. On the other hand, personal data protection, and ensuring health status or medical conditions are not mentioned, brief training or education on data security, and assuring data confidentiality and privacy were the consistent recommendations provided by patients [21, 24, 30]. These findings coincide with the suggestion by Perera [49] stating the use of an alphanumeric passcode to ensure the protection of mHealth apps rather than

using a four-digit pin, as well as wiping data from the mobile device after a specific number of failed passcode attempts [49]. Nurgalieva et al. [13] in their review also emphasised the frequency of notifications and alerts programmed into mHealth apps. Accordingly, discreet or private notification was advised to prevent any distress to users, particularly in situations where someone mistakenly views the icon. Overall, these recommendations reflect the need for users to have complete control in using their mobile device for mHealth, and avoid any intrusion into their daily life. Training and education as recommended by patients in this study corroborate the report by Lewis et al. [51] as reviewed by Nurgalieva et al. [13]. The latter authors suggested that the risk factors for violation of users' privacy and security in mHealth apps can be categorised into external and internal risks. Whereas appropriate regulation can be used to effectively minimise the internal risk factors, proper education and training are pertinent to eliminate the external risk factors.

Concerning the fourth theme, information on the factors influencing patients' views regarding data privacy and confidentiality was obtained from a few studies included in this systematic review. Examples included socio-demographic characteristics such as age, income level, marital status, previous experience with mHealth apps [30], patients' satisfaction levels [31], perceived health information sensitivity [36, 42], data type, data stage, privacy victimization experience [39, 42]. These findings are consistent with the results presented in several previous studies [52] and the contextual nature of the theory of privacy [53]. More importantly, certain adjustments to the security and privacy features of mHealth apps need to be incorporated by the app developers upon considering patients' and users' demographics. However, given the low number of studies reporting the underlying factors influencing patients' views on data privacy, confidentiality, and security issues in mHealth apps, more research is needed to elucidate the relationships.

Implications of the findings

The findings from this study have pertinent implications for mHealth app developers, healthcare professionals, and policymakers. Both healthcare professionals and mHealth app developers have a vital role to play in addressing the diverse views demonstrated by patients and end-users on data privacy, confidentiality, and security issues in mHealth apps.

While mhealth app developers are primarily responsible for designing security measures and features to ensure their data privacy and confidentiality, from the aspect of healthcare providers and patient relationships, the former plays a pivotal role in educating patients or end-users regarding such measures. This could be discussed during routine consultation, as well as reinstating the need for collecting sensitive data and what they are going to be used for. Regarding unauthorised third-party access and potential data breaches, users may benefit from information on the privacy requirements and meeting the standards set by the GDPR and HIPPA, which are designed to ensure such privacy issues and data breaches are prevented.

Apart from informing patients and end-users on the type of data to be collected and the

intended use, the aspect of training and educating end-users on the available features and measures to ensure data privacy and security cannot be overemphasised. Meanwhile, stakeholders need to gauge the users' level of awareness and knowledge of these issues, as well as the underlying reasons for the diverse views on these issues to tailor the educational interventions accordingly. As gleaned from the several studies included in this review, users' less concern about their data privacy may stem from being completely ignorant or they may perceive that the benefits of using mHealth outweigh the potential risks.

This study also has important implications for mHealth app developers given the fact that patients and end users have raised concerns about data privacy, security and confidentiality issues that end up affecting their usage of such apps [18, 32]. Nevertheless, accumulated findings reflect that patients' perceptions of privacy issues and influence their adoption of mHealth apps are context-dependent [39, 43]. Since most of the reviewed studies entailed surveys, it is expected that users will raise concerns on privacy or confidential issues relating to mHealth apps, but further enquiries are required to elucidate if such concerns influence their behaviour and actual usage of such apps. These events need to be succinctly explored in future studies, and stakeholders need to understand this grey area to effectively address the issues. In addition, mHealth app developers may digest the issues raised by users and strategize on how to improve their current security and privacy measures, particularly ensuring to meet the requirements of the HIPAA and GDPR. Furthermore, the appropriate actions to be taken by end-users in different circumstances should be clarified in the developed security policy and guidelines. In summary, providing suitable security awareness on the security guidelines and policies for end-users is as pertinent as developing secure mHealth apps.

For policymakers and researchers, this study highlights the aspects prioritised by patients for the adoption and desired outcomes of implementing mHealth apps, as well as addressing issues relating to data privacy and security. Accordingly, better patient-healthcare professional relationships, trust, personal data protection, and ensuring health status or medical conditions are not mentioned, brief training or education on data security were the consistent recommendations provided by patients (23, 24, 19). While most of the aforementioned points can be conveyed to users, trust is a feature that has to be earned, which has to be driven by healthcare providers and the government. These stakeholders also have to mitigate apprehensions relating to patients' privacy concerns to ensure enhanced trust between patients and service providers, which is crucial to the successful delivery of e-health services.

Certain concrete actions can be taken by the stakeholders at the government level by considering the HIPAA and EU safe harbour law, which advocates for strict security measures for exchanging and sharing of health data, and failure to comply with such laws is followed by severe consequences. From the healthcare providers' perspectives and given the confidentiality and sensitivity of patient data, only authorised users such as medical staff should be given access to the stored health data. Nevertheless, confidentiality and availability need to be carefully balanced when structuring this critical security system. The fact that all patient's health data are made available to be

exchanged, shared and monitored to provide robust healthcare services, certain aspects of the data may be considered confidential and for security reasons, must be kept restricted or inaccessible. These goals should be rationalised to ensure patients receive the best possible care.

Strengths and Limitations

This study involved a comprehensive systematic literature search and identification of relevant and recent articles on mHealth apps' privacy, security and confidentiality published in the last eight years. Detailed information on patients' perspectives and awareness of the privacy and security of mHealth apps were gleaned from this review, thus bridging the current research gap as no systematic review has been conducted on the aforementioned topic. Thematic and empirical analyses were also performed to obtain robust data from the various research designs employed in the articles and to triangulate the findings.

Nevertheless, the limitations of this study are well acknowledged. The literature search was restricted to three databases; thus some important articles on the research topic might be missed. Only patients and end-users were considered as the primary targets in this review, while other active stakeholders in mHealth apps, such as the perspectives of healthcare professionals, app developers, and policymakers, were not documented. The issues raised in this study might be better understood if all relevant stakeholders were considered. This event also limits the generalisability of findings as no inference could be made regarding healthcare personnel and mHealth app developers. The use of one reviewer for the data extraction is also an important limitation, however, the reviewer was trained on how to perform the data extraction and coding prior to the study to ensure the process was reproducible and consistent.

Meanwhile, a general limitation in the retrieved articles is the need for a clear definition of data privacy and security. Most of the reviewed papers considered security and privacy as a single concept, particularly as part of a general assessment of mHealth design. Although security and privacy may overlap when ensuring patients' confidentiality, the two concepts are fundamentally different. In addition, only one study assessed the relationship between patients' sociodemographic factors and their concerns regarding mHealth apps' privacy, security and confidentiality. A more robust assessment of patients' demographic characteristics, environmental factors, and their antecedents on the data breaches and leakage to unwanted third parties requires further investigation.

Conclusion

This systematic review elucidated patients' perspectives and awareness regarding mHealth apps' privacy, security and confidentiality. Patients demonstrated diverse perspectives of the trio concepts, ranging from users who were satisfied with the privacy and security features of their current mHealth apps to those who raised pertinent issues affecting the technology utilisation. Patients also conveyed specific approaches to improve the use of mHealth apps (facilitators) such as protection of personal data, ensuring the confidentiality of health status or medical condition, and

providing brief training or education on data security and privacy.

The aggregation of the empirical and thematic results reflect that these diverse perspectives might be linked to the awareness of the subject matter, which also differed across these events and was influenced by patients' sociodemographic characteristics such as age, income level, and marital status, as well as experience with mHealth apps, satisfaction levels, data type and data stage. Thus, the findings in this review may be beneficial to mHealth app developers and other stakeholders in improving patients' awareness and adjusting current privacy and security features to enhance the use and adoption of mHealth apps for routine health monitoring and management of specific health conditions.

Acknowledgements

The authors appreciate the support provided by the Institute of Digital Healthcare, University of Warwick, Coventry, United Kingdom in developing this review article.

Funding Statement

This study did not receive any funding support

Data Availability

The data sets generated during and/or analyzed during this study are available from the corresponding author on reasonable request

Conflict of Interest

The authors have no conflict of interest

Author Contributions

Conceptualization: GE, TNA, and NA, Data curation: NA and MA, Formal analysis; NA and MA, Investigation; NA and MA, Methodology: GE, TNA, and NA, Project administration: MA and NA, Resources: GE, TNA, and NA, Supervision: GE, TNA, and NA, Writing - original draft: NA, Writing - review & editing: GE, TNA, and NA

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. Lee Ventola, C. (2014) 'Mobile devices and apps for health care professionals: Uses and benefits', *Pharmacy and Therapeutics*, 39(5), pp. 356–364.
 7. Bani Issa, W. et al. (2020) 'Privacy, confidentiality, security and patient safety concerns about electronic health records', *International Nursing Review*, 67(2), pp. 218–230. doi: 10.1111/inr.12585.
 8. Tomar (2021)
 9. 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.
 10. 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.
 11. Esposito, De Santis, Tortora, Chang, & Choo, 2018
 12. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562. <https://doi.org/10.1016/j.jbi.2012.12.003>
 13. Nurgalieva, L., O'callaghan, D., Doherty G. (2016). Security And Privacy Of Mhealth Applications: A Scoping Review. *IEEE Access*, 4.
 14. Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems*, 39(1), 181. <https://doi.org/10.1007/s10916-014-0181-3>
 15. Page et al. (2021)
 16. Grant et al. (2009)
 17. Alwashmi, M. F., Fitzpatrick, B., Farrell, J., Gamble, J. M., Davis, E., Nguyen, H. V., Farrell, G., & Hawboldt, J. (2020). Perceptions of Patients Regarding Mobile Health Interventions for the Management of Chronic Obstructive Pulmonary Disease: Mixed Methods Study. *JMIR mHealth and uHealth*, 8(7), e17409. <https://doi.org/10.2196/17409>
 18. Moodley, J., Constant, D., Botha, M. H., van der Merwe, F. H., Edwards, A., & Momberg, M. (2019). Exploring the feasibility of using mobile phones to improve the management of clients with cervical cancer precursor lesions. *BMC women's health*, 19(1), 2. <https://doi.org/10.1186/s12905-018-0702-1>
 19. Bradbury, A., Patrick-Miller, L., Harris, D., Stevens, E., Egleston, B., Smith, K., Mueller, R., Brandt, A., Stopfer, J., Rauch, S., Forman, A., Kim, R., Fetzer, D., Fleisher, L., Daly, M., & Domchek, S. (2016). Utilizing Remote Real-Time Videoconferencing to Expand Access to Cancer Genetic Services in Community Practices: A Multicenter Feasibility Study. *Journal of medical Internet research*, 18(2), e23. <https://doi.org/10.2196/jmir.4564>
 20. Sangers, T. E., Wakkee, M., Kramer-Noels, E. C., Nijsten, T., & Lugtenberg, M. (2021). Views on mobile health apps for skin cancer screening in the general population: an in-depth qualitative exploration of perceived barriers and facilitators. *The British journal of dermatology*, 185(5), 961–969. <https://doi.org/10.1111/bjd.20441>

21. Gill et al., 2019
22. De Vries, S. T., Wong, L., Sutcliffe, A., Houyez, F., Ruiz, C. L., Mol, P. G., & IMI Web-RADR Work Package 3b Consortium (2017). Factors Influencing the Use of a Mobile App for Reporting Adverse Drug Reactions and Receiving Safety Information: A Qualitative Study. *Drug safety*, 40(5), 443–455. <https://doi.org/10.1007/s40264-016-0494-x>
23. Hackett, K. M., Kazemi, M., & Sellen, D. W. (2018). Keeping secrets in the cloud: Mobile phones, data security and privacy within the context of pregnancy and childbirth in Tanzania. *Social science & medicine* (1982), 211, 190–197. <https://doi.org/10.1016/j.socscimed.2018.06.014>
24. 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>
25. Wyatt, K. D. et al. (2020) 'Patients' experiences and attitudes of using a secure mobile phone apps for medical photography: Qualitative survey study', *Journal of Medical Internet Research*, 22(5), p. e14412. doi: 10.2196/14412.
26. 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.
27. Alaiad, A., Alsharo, M. and Alnsour, Y. (2019) 'The Determinants of M-Health Adoption in Developing Countries: An Empirical Investigation', *Applied Clinical Informatics*, 10(5), pp. 820–840. doi: 10.1055/s-0039-1697906.
28. Özkan, Ö., Aydin Son, Y. and Aydinoglu, A. U. (2019) 'Security and Privacy Concerns Regarding Genetic Data in Mobile Health Record Systems: An Empirical Study from Turkey', *bioRxiv*, June, p. 678912. doi: 10.1101/678912.
29. Glauser, G. et al. (2019) 'Assessing the utility of an IoS application in the perioperative care of spine surgery patients: the NeuroPath Pilot study', *mHealth*, 5(40), pp. 1–6. doi: 10.21037/mhealth.2019.09.01.
30. 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.
31. Barutçu, S., Barutçu, E. and Adigüzel, D. Ü. (2018) 'A Technology Acceptance Analysis for mHealth Apps: The Case of Turkey', *Balkan and Near Eastern Journal of Social Sciences*, 4(4), pp. 104–113.
32. Bauer, A. M. et al. (2018) 'Acceptability of mHealth augmentation of Collaborative Care: A mixed-methods pilot study', *General Hospital Psychiatry*. Elsevier, 51, pp. 22–29. doi: 10.1016/j.genhosppsych.2017.11.010.
33. Goetz, M. et al. (2017) 'Perceptions of patient engagement applications during pregnancy: A qualitative assessment of the patient's perspective', *JMIR Mhealth Uhealth*, 5(5), p. e73. doi: 10.2196/mhealth.7040.
34. Richardson, J. E. and Ancker, J. S. (2015) 'Public Perspectives of Mobile Phones' Effects on Healthcare Quality and Medical Data Security and Privacy: A 2-Year Nationwide Survey', *Annual Symposium proceedings*, pp. 1076–1082.
35. Sanger, P. et al. (2014) 'Design Considerations for Post-Acute Care mHealth: Patient Perspectives', *Annual Symposium proceedings*, 2014, pp. 1920–1929.
36. 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>
37. Biswas, M., Tania, M. H., Kaiser, M. S., Kabir, R., Mahmud, M., & Kemal, A. A. (2021). ACCU3RATE: A mobile health application rating scale based on user reviews. *PloS one*, 16(12), e0258050. <https://doi.org/10.1371/journal.pone.0258050>
 38. Casilang, C. G., Stonbraker, S., Japa, I., Halpern, M., Messina, L., Steenhoff, A. P., Lowenthal, E. D., & Fleisher, L. (2020). Perceptions and Attitudes Toward Mobile Health in Development of an Exclusive Breastfeeding Tool: Focus Group Study with Caregivers and Health Promoters in the Dominican Republic. *JMIR paediatrics and parenting*, 3(2), e20312. <https://doi.org/10.2196/20312>
 39. 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>
 40. Harris, B., Ajisola, M., Alam, R. M., Watkins, J. A., Arvanitis, T. N., Bakibinga, P., Chipwaza, B., Choudhury, N. N., Kibe, P., Fayehun, O., Omigbodun, A., Owoaje, E., Pemba, S., Potter, R., Rizvi, N., Sturt, J., Cave, J., Iqbal, R., Kabaria, C., ... Griffiths, F. (2021). Mobile consulting as an option for delivering healthcare services in low-resource settings in low- and middle-income countries: A mixed-methods study. *DIGITAL HEALTH*. <https://doi.org/10.1177/2055207621103342541>
 41. Al-Anezi F. M. (2021). Evaluating the Readiness of Mobile Technology with Respect to e-Health for Medication in Saudi Arabia: An Integrative Perspective. *Journal of multidisciplinary healthcare*, 14, 59–66. <https://doi.org/10.2147/JMDH.S287321>
 42. Ermakova, T., Fabian, B., & Zarnekow, R. (2016). Improving Individual Acceptance of Health Clouds through Confidentiality Assurance. *Applied clinical informatics*, 7(4), 983–993. <https://doi.org/10.4338/ACI-2016-07-RA-0107>
 43. Rodrigues, R., Poongulali, S., Balaji, K., Atkins, S., Ashorn, P., & De Costa, A. (2015). 'The phone reminder is important, but will others get to know about my illness?' Patient perceptions of an mHealth antiretroviral treatment support intervention in the HIVIND trial in South India. *BMJ Open*, 5(11), e007574. <https://doi.org/10.1136/bmjopen-2015-007574>
 44. Al-Mahrouqi, T., Al-Alawi, K., Al-Alawi, M., Al Balushi, N., Al Ghailani, A., Al Sabti, H., & Al Sinawi, H. (2022). A promising future for tele-mental health in Oman: A qualitative exploration of clients and therapists' experiences. *SAGE open medicine*, 10, 20503121221086372. <https://doi.org/10.1177/20503121221086372>
 45. Turcotte, V., Chagnon, A., & Guénette, L. (2021). Experience and perspectives of users and non-users of the Ask your pharmacist teleconsultation platform. *Exploratory research in clinical and social pharmacy*, 2, 100031.
 46. Morton et al. (2021)
 47. Cavazos-Rehg, P., Min, C., Fitzsimmons-Craft, E. E., Savoy, B., Kaiser, N., Riordan, R., Krauss, M., Costello, S., & Wilfley, D. (2020). Parental consent: A potential barrier for underage teens' participation in an mHealth mental health intervention. *Internet interventions*, 21, 100328. <https://doi.org/10.1016/j.invent.2020.100328>
 48. Hattingh, H. L., Knox, K., Fejzic, J., McConnell, D., Fowler, J. L., Mey, A., Kelly, F., &

- Wheeler, A. J. (2015). Privacy and confidentiality: perspectives of mental health consumers and carers in pharmacy settings. *The International journal of pharmacy practice*, 23(1), 52–60. <https://doi.org/10.1111/ijpp.12114>
49. Perera C (2012). Principles of Security for the use of Mobile Technology in Medicine. *J Mob Technology Med*; **1**: 5-7 [DOI: 10.7309/jmtm10]
50. 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]
51. Krebs P & Duncan DT (2015). Health app use among US mobile phone owners: a national survey. *JMIR Mhealth UHealth*, Nov;3(4):e101 [FREE Full text] [doi: 10.2196/mhealth.4924]
52. 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]
53. Nissenbaum H. (2004). Privacy as contextual integrity. *Wash Law Rev*;79(1):101-139
- 54.**