

Consumer Trust and Privacy Concerns in the Adoption of Digital Health Services: a Systematic Review

Sushil Pal^{1*}, Shivam Agarwal², Hemant Kumar³, Sharad Kumar⁴, Archana Rani⁵

¹Charak Institute of Allied and Healthcare Studies Lucknow, Uttar Pradesh, India.

Email Id:- upsushilpal1999@gmail.com

²College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, U.P. India.

Email Id:- shivamagarwal50283@gmail.com

³College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, U.P. India.

Email ID:- hemantkurmi53498@gmail.com

⁴School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

Email ID:- sharadkumar6788@gmail.com

⁵School of Health and Paramedical Sciences, Vivek University, Bijnor, Uttar Pradesh, India.

Email ID:- chauhanarchana002@gmail.com

*Coessponding Author

Sushil Pal

Charak Institute of Allied and Healthcare Studies Lucknow, Uttar Pradesh, India

Email ID: upsushilpal1999@gmail.com

. \

ABSTRACT

Digital health services have become an important part of healthcare delivery, but consumer trust and privacy concerns may influence their acceptance and continued use. This review examined the relationship between these factors and digital health adoption. Original studies published between January 2020 and December 2025 were considered through targeted literature searches. Five studies were selected for preliminary narrative analysis, focusing on consumer trust, privacy concerns, service characteristics and adoption-related outcomes. Comprehensive database screening and formal quality assessment remain incomplete. The findings indicated that trust in healthcare professionals, service providers and digital platforms was generally associated with greater willingness to use digital health services. However, the relationship between privacy concerns and adoption was inconsistent. Some studies reported negative associations, while others found no significant direct relationship. Perceived benefits, control over personal information and confidence in service providers also appeared relevant to consumer decisions. Most studies examined self-reported intentions rather than actual usage, limiting conclusions about long-term engagement. Overall, trust and privacy concerns appear relevant to digital health acceptance, although their influence varies across settings and populations. Further systematic investigation is needed to clarify these relationships and their implications for sustained digital health use

Keywords: Digital health; consumer trust; privacy concerns; technology adoption; telemedicine

INTRODUCTION

Choosing a digital health service involves more than deciding whether an application is convenient. Users may also need to judge who can access their information, how it will be used and whether the Organisation delivering the service is dependable (1). Empirical research in healthcare has incorporated trust and privacy into models of technology acceptance, extending the usual emphasis on usefulness and ease of use (1,2). These additions are particularly relevant when a service requires the disclosure of symptoms, treatment histories or other personal information. Trust requires a clear object. Confidence in a clinician is conceptually different from confidence in a commercial platform or in the safeguards

surrounding a service. Privacy also includes several distinct issues: concern about disclosure, perceived likelihood of misuse and the degree of control a person believes they retain over their data (3). Research on mobile health has examined security-related barriers, while privacy-calculus models consider how perceived benefits and information-related concerns enter the same decision (3,4) These concepts should be defined separately before their associations are compared. A further distinction concerns the outcome being explained. Willingness to try a service is an initial intention; an intention to continue arises after experience. Telemedicine research has explicitly examined the latter and has differentiated several forms of trust (5). A questionnaire response does not, by itself, establish that a

person downloaded an application, completed a consultation or remained an active user. Combining these outcomes under a single adoption label can obscure what the evidence actually supports. General acceptance models may not explain all service contexts equally well. Research comparing lifestyle and therapy applications has questioned the adequacy of an extended acceptance model, while newer qualitative work has examined how users understand artificial intelligence in consumer-facing health applications (6,7). A related systematic review already addresses patients' perspectives on mobile health privacy, security and confidentiality (8). The intended contribution of the present review is therefore a focused examination of the relationships between trust, privacy and distinct stages of adoption. The review question is: among adult users or potential users of patient-facing digital health services, how are consumer trust and privacy concerns associated with adoption intention, actual uptake and continued use? Secondary questions concern the target of trust, the privacy construct measured and differences between service settings.

MATERIALS AND METHODS

This systematic review was designed following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines. The search strategy covers three electronic databases—PubMed, Scopus, and Web of Science—to identify relevant original research articles published between January 2020 and December 2025. Search terms include “digital health,” “mHealth,” “telemedicine,” “telehealth,” “consumer trust,” “privacy concerns,” “data security,” “perceived

privacy risk,” “technology adoption,” “user acceptance,” and “continuance intention,” combined using the Boolean operators AND and OR. Preliminary searches were conducted through accessible PubMed records and publisher websites; comprehensive database searches remain to be completed. Eligible studies will include freely accessible, English-language original quantitative, qualitative, and mixed-methods research examining the relationship of trust or privacy concerns with the adoption or continued use of digital health services among adults aged 18 years and older. Review articles, conference abstracts without full reports, duplicate publications, and studies unrelated to consumer adoption will be excluded. Two reviewers will independently screen titles, abstracts, and full texts, with disagreements resolved through discussion. Relevant study characteristics and findings will be extracted and synthesized narratively, considering differences in study design, digital health services, and outcome measures. The completed identification and selection process will be presented using a PRISMA 2020 flow diagram.

RESULTS

Overview of the Preliminary Evidence

Five original studies published between 2020 and 2025 were identified for this preliminary evidence assessment. The evidence comprised quantitative surveys, structural equation modelling, and qualitative interviews conducted in India, Germany, China, and the United States. The studies differed in their participant characteristics, service types, and measures of adoption or continued use (Table 1)

. Table 1. Characteristics and key findings of selected original studies

Study	Country and design	Sample	Principal findings
Dhagarra et al., 2020 (1)	India; cross-sectional survey and structural equation modelling	416	Trust was positively associated with intention to accept healthcare technology, whereas privacy concerns showed a negative association.
Schomakers et al., 2022 (6)	Germany; online survey comparing lifestyle and therapy mHealth apps	707	Trust predicted intention to use therapy apps but not lifestyle apps; privacy concerns were not significant predictors in the tested model.
von Kalckreuth and Feufel, 2023 (4)	Germany; vignette-based survey and structural equation modelling	250	Provider trust and perceived benefits were associated with intention to use mHealth apps; privacy concerns showed no significant direct association.
Zhu et al., 2023 (5)	China; telemedicine questionnaire and structural equation modelling	465	Different dimensions of trust were related to continuance intention; privacy concerns negatively moderated the association between structural assurance-based trust and continuance intention.
Ryan et al., 2025 (7)	United States; qualitative interviews concerning AI-enabled mHealth	21	Participants discussed professional endorsement, institutional trust, personal data collection, information sharing, and potential future uses of health data.

The preliminary evidence indicates that consumer trust is associated with the intention to use digital health services, although the strength and nature of this relationship vary across settings. Dhagarra et al. (1) reported a positive relationship between trust and healthcare technology acceptance among patients in India. Similarly, von Kalckreuth and Feufel (4) identified provider trust and perceived benefits as factors associated with mHealth adoption intention. Schomakers et al. (6) found that trust was associated with intention to use therapy applications but not lifestyle applications. These findings suggest that the relevance of trust may depend on the intended purpose of the digital health service and the institution or technology being trusted.

Privacy Concerns and Continued Use

Findings concerning privacy were less consistent. Dhagarra et al. (1) observed a negative association between privacy concerns and behavioural intention, whereas von Kalckreuth and Feufel (4) found no significant direct relationship in their model. The latter study also identified relationships between perceived control over personal data, privacy concerns, and provider trust. Schomakers et al. (6) similarly reported no significant predictive contribution of privacy concerns to usage intention in their tested model. In contrast, Zhu et al. (5) found that privacy concerns negatively moderated the relationship between structural assurance-based trust and telemedicine continuance intention. These differences indicate that privacy-related findings should be interpreted according to the measures used and whether the outcome concerns initial acceptance or continued use.

Qualitative Findings and Overall Synthesis

The qualitative investigation by Ryan et al. (7) provided additional perspectives on trust and privacy in AI-enabled mobile health services. Participants raised questions about the credibility of technology providers, professional endorsement, the collection of personal information, and its potential future use. These findings complement the quantitative evidence but do not provide estimates of adoption effects. Overall, the preliminary literature indicates that trust, privacy concerns, perceived benefits, and control over personal information are relevant to understanding digital health acceptance. However, variation in research designs, service contexts, and outcome measures limits direct comparison. Further systematic screening, data extraction, and methodological appraisal are necessary before drawing conclusions about the consistency or magnitude of these relationships.

DISCUSSION

The preliminary findings suggest that consumer trust and privacy concerns play important roles in digital health adoption, although their relationships with acceptance vary across healthcare settings and technologies. Dhagarra et al. (1) reported a positive association between trust and behavioural intention, while privacy concerns were negatively associated with healthcare technology acceptance. In contrast, von Kalckreuth and Feufel (4) observed that provider trust and perceived benefits were associated with adoption intention, whereas privacy concerns showed no significant direct relationship. These differences suggest that consumers

consider several factors when deciding whether to use digital health services. The influence of trust and privacy may therefore depend on the type of service, previous healthcare experiences and users' expectations. Trust may also differ according to whether it concerns healthcare professionals, digital platforms or the institutions responsible for managing personal information. Zhu et al. (5) examined different dimensions of trust among telemedicine users and found associations with continuance intention. Their findings suggest that patients may distinguish between confidence in a physician and confidence in the technology used to deliver healthcare. Schomakers et al. (6) also examined acceptance across different categories of mobile health applications, highlighting the need to consider service context when interpreting consumer attitudes. These observations indicate that trust should not be treated as a uniform concept across digital healthcare services. Privacy concerns present a more complex relationship with digital health adoption. Although concerns about unauthorized access, information sharing and misuse of personal health data may discourage some users, their influence is not consistent across studies. Von Kalckreuth and Feufel (4) found no significant direct association between privacy concerns and adoption intention in their model, whereas Zhu et al. (5) reported that privacy concerns negatively moderated the relationship between structural assurance-based trust and telemedicine continuance intention. These findings suggest that perceived control over personal information and confidence in service providers may be important when interpreting privacy-related attitudes. Clear data protection policies, understandable consent procedures and transparent information-sharing practices warrant further evaluation as possible ways to address consumer concerns. The increasing use of artificial intelligence in healthcare has introduced additional questions about the reliability of digital services and the protection of sensitive information. Ryan et al. (7) explored consumer perspectives on AI-enabled mobile health applications and identified concerns involving professional endorsement, personal data collection and potential future uses of health information. Such findings indicate that trust may extend beyond technical performance to include transparency and accountability. However, qualitative perceptions cannot establish the extent to which these concerns influence actual service use. Furthermore, Alhammad et al. (8) previously reviewed patients' perspectives on privacy, confidentiality and security in mobile health applications (9). The present review seeks to extend this discussion by examining the relationships of trust and privacy concerns with different stages of adoption, particularly initial acceptance and continued use. Several limitations should be considered when interpreting the present findings. The evidence assessment was preliminary, and comprehensive searches of PubMed, Scopus and Web of Science have not yet been completed. The selected studies differed in their populations, research designs, digital health services and outcome measures, limiting direct comparisons. Most quantitative studies assessed self-reported intentions rather than actual adoption or sustained use, making causal interpretation inappropriate. In addition, independent screening, complete data extraction and formal methodological quality assessment remain outstanding. Restricting the completed review to freely accessible English-language publications may introduce selection bias. Consequently, the current findings should be interpreted

cautiously until the systematic review procedures have been completed.

CONCLUSION

The preliminary findings suggest that consumer trust and privacy concerns are relevant to the adoption and continued use of digital health services, although their associations vary across healthcare settings and technologies. Trust in healthcare providers and digital platforms was generally associated with greater adoption intention, while findings concerning privacy were inconsistent. Differences in study designs, service types and outcome measures limit firm conclusions. Further systematic evaluation and longitudinal research are needed to clarify these relationships and determine how trust and privacy concerns influence actual digital health use.

REFERENCES

1. Dhagarra D, Goswami M, Kumar G. Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. *Int J Med Inform*. 2020;141:104164. doi:10.1016/j.ijmedinf.2020.104164. Free full text: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7212948/>
2. Deng Z, Hong Z, Ren C, Zhang W, Xiang F. What predicts patients' adoption intention toward mHealth services in China: empirical study. *JMIR Mhealth Uhealth*. 2018;6(8):e172. doi:10.2196/mhealth.9316. Free full text: <https://mhealth.jmir.org/2018/8/e172/>
3. Zhou L, Bao J, Watzlaf V, Parmanto B. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. *JMIR Mhealth Uhealth*. 2019;7(4):e11223. doi:10.2196/11223. Free full text: <https://mhealth.jmir.org/2019/4/e11223/>
4. von Kalckreuth N, Feufel MA. Extending the privacy calculus to the mHealth domain: survey study on the intention to use mHealth apps in Germany. *JMIR Hum Factors*. 2023;10:e45503. doi:10.2196/45503. Free full text: <https://humanfactors.jmir.org/2023/1/e45503/>
5. Zhu L, Jiang X, Cao J. Factors affecting continuance intention in non-face-to-face telemedicine services: trust typology and privacy concern perspectives. *Healthcare (Basel)*. 2023;11(3):374. doi:10.3390/healthcare11030374. Free full text: <https://pmc.ncbi.nlm.nih.gov/articles/PMC9914105/>
6. Schomakers EM, Lidynia C, Vervier LS, Calero Valdez A, Ziefle M. Applying an extended UTAUT2 model to explain user acceptance of lifestyle and therapy mobile health apps: survey study. *JMIR Mhealth Uhealth*. 2022;10(1):e27095. doi:10.2196/27095. Free full text: <https://mhealth.jmir.org/2022/1/e27095/>
7. Ryan K, Hogg J, Kasun M, Kim JP. Users' perceptions and trust in AI in direct-to-consumer mHealth: qualitative interview study. *JMIR Mhealth*

DECLARATIONS

- Ethics Approval and Consent to Participate: Not applicable, as this review does not involve direct human participation or collection of primary data.
- Consent for Publication: Not applicable.
- Funding: No funding was received for this study.
- Competing Interests: The authors declare no competing interests.
- Author Contributions: All authors contributed to the conceptualization, literature review, manuscript preparation, critical revision, and approval of the final manuscript.
- Data Availability: All information discussed in this review was obtained from previously published studies. No new datasets were generated.

Uhealth. 2025;13:e64715. doi:10.2196/64715. Free full text: <https://mhealth.jmir.org/2025/1/e64715/>

8. Alhammad N, Alajlani M, Abd-alrazaq A, Epiphaniou G, Arvanitis T. Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: systematic review. *J Med Internet Res*. 2024;26:e50715. doi:10.2196/50715. Free full text: <https://www.jmir.org/2024/1/e50715/>

9. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*. 2021;372:n71. doi:10.1136/bmj.n71. Free full text: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8005924>