Intelligent Human Systems Integration (IHSI), Vol. 200, 2026, 140–147
https://doi.org/10.54941/ahfe1007073

Exploring Privacy in Digital Mental Health: User and Psychotherapist Perspectives

Abdulmajeed Alqhatani

Department of Information Systems, College of Computer Science & Information Systems, Najran University, Najran 61441, Saudi Arabia

ABSTRACT

The rapid adoption of psychological consultation applications in Saudi Arabia has created both opportunities for accessible mental health support and challenges related to data privacy and security. Through 13 semi-structured interviews with users and psychotherapists, this study explores privacy behaviors, concerns, and protective practices regarding psychological consultation applications. The findings reveal that most users have limited concern for privacy when engaging with psychological applications, largely placing their trust in the platforms because of their perceived legitimacy and official approval. Users also rarely read privacy policies and typically relied on basic protective measures, such as using strong passwords, to safeguard their personal information. Psychotherapists emphasized adherence to professional integrity, ethical guidelines, and regulatory requirements. The findings from this study highlight the importance of raising user awareness about privacy policies, enhancing regulatory frameworks for digital health platforms, and integrating cybersecurity best practices. Such measures are critical for ensuring the long-term sustainability of digital mental health services.

Keywords: Privacy, Security, Trust, Digital health, Psychological consultation apps, Digital mental health

INTRODUCTION

Digital technology is transforming how healthcare is delivered, enabling individuals to gain medical assistant, advice, and monitoring via smartphone apps and online sites. As these services become more mainstream, they also require collecting and storing personal health information. This raises important concerns about privacy; specifically, who has access to this information, how it is used, and whether patients feel comfortable sharing such personally sensitive information. Therefore, understanding privacy in digital health is crucial for trust and driving usage of these services.

Experience-based evidence shows a high level of privacy issues. For instance, in the United States alone, over 133 million health records were exposed in data breaches in 2023, on hospitals, clinics and insurance companies (HIPAA Journal, 2025). Surveys also reveal that people are more likely to adopt digital health apps if they feel that their information is protected, understand how their data will be used, and have the option to delete or control it (Gupta et al., 2023). These examples demonstrate that privacy plays a role in people's trust and use of digital health technologies.

Received October 2, 2025; Revised November 28, 2025; Accepted December 13, 2025; Available online February 1, 2026

This study explores privacy in psychological consultation apps, from both users and psychotherapists perspective, focusing on the Saudi Arabian context. The reminder of this paper is organized as follows: the following section reviews previous studies about privacy in digital health. It is succeeded by this study methodology and results. Finally, the paper provides a short discussion of the findings and a conclusion.

BACKGROUND

Studies on digital mental health services repeatedly draw attention to the serious privacy issues that impact user's trust, data security, and ethical practice in delivering psychological support. Alqahtani and Orji (2020) examined user reviews of mental health apps and identified some common concerns related to data handling, which undermined users' confidence in the privacy and reliability of digital mental health platforms. A comparable sentiment comes through in the study by O'Loughlin et al. (2019), who conducted a large-scale evaluation of depression apps and found that very few indicate transparent or comprehensive privacy disclosures. Their work shows that many apps fail to adequately explain what data they collect, where the data is kept, and with whom the data is shared with.

A similar line of research focuses on the readability and usability of privacy policies. Tabassum et al. (2018) showed that most traditional privacy policies are complex and rarely read by users, proposing alternative, more visual formats such as comics to enhance user comprehension. This aligns with recent findings by Alqhatani (2024), who analyzed privacy policies of psychological consultation apps in Saudi Arabia and concluded that policies were often vague, lacked clear explanations of data handling purposes, and did not explicitly describe retention or deletion practices. These studies collectively suggest that poor privacy communication is a structural issue in digital mental health ecosystems.

Research has also linked privacy concerns to user engagement and willingness to disclose sensitive information. Zhang et al. (2022) found that anxiety would considerably diminish trust toward mHealth platforms and further influence levels of openness during sessions. Their research indicated that strong social cues, such as a feeling of human presence, could mitigate some privacy fears, and thus enhancing the overall consultation experience. In contrast, other studies emphasized the risks of emerging AI-driven mental health tools. Rubeis (2022), for example, discussed the ethical and privacy implications of iHealth technologies that rely on continuous monitoring and real-time data mining. Such systems may offer therapeutic benefits, but present deep concerns about the medicalization of everyday life and the long-term storage of sensitive psychological data. Similarly, De Freitas et al. (2023) highlighted the safety and privacy risks of generative-AI companion chatbots, revealing real-world failures in crisis recognition and inappropriate responses when engaged in mental health conversations.

From a regulatory perspective, Torous et al. (2022) argued that existing oversight frameworks for digital mental health apps are inadequate because they were designed for traditional medical devices rather than fast-changing software. This regulatory gap allows many mental health apps to operate with limited transparency, inconsistent privacy safeguards, and varying degrees of accountability. Camacho et al. (2022) further noted that app-store ratings do not meaningfully reflect privacy protections and proposed specialized evaluation frameworks that include security and privacy criteria.

Overall, the current literature tends to coalesce around several key themes: privacy policies are often incomplete or difficult to understand; users' trust and behavior are strongly shaped by perceptions of institutional legitimacy; and the rapid expansion of AI-based mental health services introduces new privacy risks that exceed current regulatory capacity. Despite these advances, prior research has rarely examined privacy perceptions within culturally specific context. The present study addresses this gap by exploring how both users and psychotherapists understand and navigate privacy in locally used digital consultation platforms, offering participant-driven insights that complement policy- and system-level analyses in the existing literature.

SEMI-STRUCTURED INTERVIEW

This study uses a qualitative research method through semi-structured interviews to explore privacy perceptions and behaviors among users and psychotherapists of psychological consultation applications in Saudi Arabia. A total of 13 participants were recruited, including four psychotherapists (two males & two females) and eight female users. Participants were recruited through social media advertisements, personal contacts, and snowball sampling. All interviews were conducted over the phone to provide flexibility, comfort, and convenience for participants. Each interview lasted, on average, 10 minutes. Table 1 below summarizes interview participants information. The study is approved by the university Research Ethics Committee.

Table 1: Sample human systems integration test parameters (Folds et al., 2008).

Participant Type	#	Gender	Age	Major/Job
User	P1	Female	22	Bachelor student specializing in Phycology
	P2	Female	19	Bachelor student specializing in Phycology
	P3	Female	20	Bachelor student specializing in Phycology
	P4	Female	20	Bachelor student specializing in Phycology
	P5	Female	23	Bachelor student specializing in Phycology
	P6	Female	39	University professor specializing in Psychology
	P7	Female	20	Bachelor student specializing in Phycology
	P8	Female	21	Bachelor student specializing in Phycology
Consultant/ psychotherapist	P9	Male	45	Senior Psychologist
	P10	Female	41	Psychotherapist
	P11	Male	40	Psychotherapist
	P12	Female	37	Psychologist

The interview protocol was divided into three parts. The first part covered general questions about participants' use of psychological/mental health apps, such as the types of applications used, frequency of use, and reasons for choosing these platforms. The second part focused on privacy concerns and protective behaviors, addressing aspects such as data sharing, trust in the apps and professionals, and actions taken to safeguard personal information. The final part gathered demographic information including age, gender, and professional background to contextualize the responses. The semi-structured interview format allowed flexibility for probing follow-up questions and clarifications when participants raised new or relevant issues.

All interviews were transcribed and analyzed using an open coding approach supported by qualitative data analysis software. The analysis process involved reading the transcripts to identify key ideas, recurring concepts, and meaningful patterns. Initial codes were refined and grouped into broader themes that captured shared and contrasting views between users and psychotherapists. This open coding approach enabled the researcher to generate insights directly from participants' experiences, ensuring that findings remained grounded in their own perspectives and expressions.

However, this study presents two main limitations. First, the sample lacked diversity in its participants, as all user participants were female and most were young adults. Second, this study is based on self-reported data and might have failed to capture accurate or comprehensive information about participants' actual privacy behaviors.

FINDINGS

This study examined privacy behaviors, concerns, and protective practices among users and psychotherapists who engage with psychological consultation applications in Saudi Arabia. The findings are organized into two main thematic areas: (1) general use and perceptions of psychological consultation apps, and (2) privacy attitudes and practices.

General Use of Psychological Consultation Applications

Users reported turning to psychological consultation apps primarily to address emotional distress, academic stress, or curiosity. Several users sought help for depression or family-related issues, while others wanted brief professional advice regarding school pressure or personal well-being. A few participants used the apps out of curiosity to explore how online consultations work. These motivations reflect the growing reliance on digital platforms as accessible and convenient sources of psychological support in the Saudi context.

Most users reported limited engagement with the apps, often using them only once or a few times. A notable exception was a user who consulted the platform multiple times over two months. Psychotherapists, however, interacted with the platforms frequently, in some cases conducting three to four sessions per day. This contrast highlights differing levels of familiarity and engagement between users and service providers.

Users commonly provided basic personal information such as name, mobile number, email, national ID, and age. Some also shared additional details (e.g., height or length), though these were not clinically necessary. Users often believed that certain information, such as age or date of birth was required for treatment planning or identity verification. Consultants confirmed that they sometimes request clinical details like family history, but emphasized that such information is sought only to support therapeutic assessment and planning.

Privacy Behaviors, Concerns, and Protective Practices

Across interviews, users expressed a strong sense of trust in psychological consultation apps, frequently citing their approval by the Ministry of Health, reputation, or perceived professionalism. Many users believed that the apps would not misuse their personal information. As a result, privacy concerns were generally low. Even when acknowledging possible data breaches, users felt that they did not share sufficiently sensitive information to pose personal risk.

Most users reported that they did not fully read privacy policies. Even those who skimmed the policies did not engage with them in detail. Only one user indicated that she carefully reviewed the privacy policy prior to using the app. This behavior reinforces the pattern of low privacy awareness and limited critical evaluation of data handling practices.

With respect to protective measures, users relied on simple security measures, such as using strong passwords or avoiding sharing sensitive information. Many users took no additional protective steps and assumed that the app's internal security protections were sufficient. On the other hand, psychotherapists reported that the platforms employ dedicated cybersecurity teams to monitor and defend against security threats. They also noted features, such as the privacy of psychological test results, which are only accessible to consultants if voluntarily shared by the client. These insights reflect stronger privacy awareness among consultants compared to users.

However, psychotherapists emphasized adherence to ethical and professional standards, including strict confidentiality, compliance with regulatory requirements, and the obligation to protect patient information. Consultants noted that information, such as personal contact information is not visible to therapists. Additional information, such as family history is requested only to support treatment. Consultants also noted that Licensed psychotherapists must pass professional ethics examinations that include privacy-related content. Psychotherapists also indicated that patient information may only be disclosed in exceptional cases involving life-threatening risks, such as suicidal intent, where disclosure is necessary to ensure client safety.

DISCUSSION

The findings of this study suggest some key insights to the way users and psychotherapists in Saudi Arabia view and manage privacy when interacting with psychological consultation applications. While these services are becoming more relevant for low threshold psychological support, the findings confirm a gap between perceived and actual privacy awareness among users, alongside stronger regulatory adherence by psychotherapists.

A key observation is the lack of privacy concern among users, who generally trusted the platforms without critically evaluating their data practices. The trust placed in the institution would seem to lower users' perceptions of risk, even while disclosing personal information. This trust-oriented behavior is consistent with other previous research that demonstrates that digital health or government service-users often assume strong privacy protections, even in the absence of a review of policy details or an evaluation of platform security (Ostherr et al., 2017). Particularly in the case of psychological consultation apps that disclose intimate emotional or behavioral information, this strong orientation towards institutional trust may present users with privacy risks they are unaware of.

Another finding relates to limited engagement with privacy policies. The majority of users did not read privacy policies, or only skimmed through them superficially, a phenomenon that is commonly reported in the digital privacy literature (Isabel Wagner, 2022). Privacy policies for mental health applications typically contain crucial information regarding data sharing, storage practices, third-party involvement, and potential risks. Mental health app privacy policies often include important information about data sharing and storage practices, third party involvement, and risk. The participant who mentioned reading the policy in detail represents an exception rather than a trend, re-emphasizing the necessity for better tactics to make privacy information clearer, more accessible, and more user-friendly.

In contrast to users, psychotherapists perceived themselves as more aware of their privacy obligations and regulatory requirements. Therapists stressed ethical obligations, confidentiality norms, and compliance with existing guidelines. Their understanding of when to share data, like in instances of imminent harm, also suggests that they are rooted in professional ethics. This contrast highlights a gap in privacy literacy: psychotherapists have professional and regulatory knowledge, while users rely primarily on trust and wishful thinking.

The findings also point to simple protective behaviors among users, such as using strong passwords or choosing not to disclose highly sensitive personal information. These actions do demonstrate some care, but do not go far enough in privacy protection. Users rarely engaged in more sophisticated protective behaviors, such as verifying data permissions, reviewing application settings, or limiting data access. This limited behavioral response suggests that users may not fully understand the sensitivity of psychological data or the potential implications of misuse. Given the sensitivity of mental health data, promotion of privacy literacy is important.

In sum, these findings suggest a critical need for awareness campaigns and better regulations. The reliance of the users on legitimization can be utilized for an improvement in risk communication. For example, apps could implement more user-friendly privacy summaries, visual indicators of data use, or mandatory brief privacy tutorials before first use. Regulators could also consider standardizing privacy requirements for digital mental health platforms to ensure consistent protections across providers. With the growing demand for online psychosocial support services in Saudi Arabia, it is crucial to have better regulatory enforcement on this category of apps, accompanied by user education and clear communication to build digital trust.

CONCLUSION

This study investigated privacy behaviors, concerns, and practices among users and psychotherapists of psychological consultation applications in Saudi Arabia. The findings reveal a gap between user trust and actual privacy awareness. While users generally expressed high confidence in the legitimacy and security of these platforms, their limited engagement with privacy policies and reliance on minimal protective measures indicate a need for stronger privacy literacy. In contrast, psychotherapists demonstrated a clearer understanding of ethical responsibilities, confidentiality requirements, and regulatory obligations, reflecting more informed privacy practices. Together, these findings highlight the importance of enhancing user education, improving transparency around data practices, and strengthen regulatory frameworks to ensure the safe and sustainable use of digital mental health services.

REFERENCES

Alqahtani, F., & Orji, R. (2020). Insights from user reviews to improve mental health apps. *Health informatics journal*, *26*(3), 2042–2066.

Alqhatani, A. (2024). Privacy Policy Analysis and Evaluation of Mobile Psychological Consultation Services in Saudi Arabia. *Human Interaction and Emerging Technologies (IHIET 2024)*, *1*(1).

Camacho, E., Cohen, A., & Torous, J. (2022). Assessment of mental health services available through smartphone apps. *JAMA Network Open*, *5*(12), e2248784–e2248784.

De Freitas, J., Uğuralp, A. K., Oğuz-Uğuralp, Z., & Puntoni, S. (2024). Chatbots and mental health: Insights into the safety of generative AI. *Journal of Consumer Psychology*, *34*(3), 481–491.

Gupta, R., Iyengar, R., Sharma, M., Cannuscio, C. C., Merchant, R. M., Asch, D. A., ... & Grande, D. (2023). Consumer views on privacy protections and sharing of personal digital health information. *JAMA network open*, *6*(3), e231305–e231305.

HIPAA Journal (2025) *Steve Alder – The HIPAA Journal*. Website: https://www.hipaajournal.com/author/hipaajournal/

Ostherr, K., Borodina, S., Bracken, R. C., Lotterman, C., Storer, E., & Williams, B. (2017). Trust and privacy in the context of user-generated healt*h data. Big Data & Soci*ety, 4(1), 2053951717704673.

O'Loughlin, K., Neary, M., Adkins, E. C., & Schueller, S. M. (2019). Reviewing the data security and privacy policies of mobile apps for depre*ssion. Internet in*terventions, 15, 110–115.

Rubeis, G. (2022). iHealth: The ethics of artificial intelligence and big data in mental healthcare. *Internet interventions*, *28*, 100518.

Tabassum, M., Alqhatani, A., Aldossari, M., & Richter Lipford, H. (2018, April). Increasing user attention with a comic-based policy. In *Proceedings of the 2018 chi conference on human factors in computing systems* (pp. 1-6).

Torous, J., Stern, A. D., & Bourgeois, F. T. (2022). Regulatory considerations to keep pace with innovation in digital health products. *Npj Digital Medicine*, *5*(1), 121.

Wagner, I. (2022). Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996--2021. *arXiv preprint arXiv:2201.08739*.

Zhang, J., Luximon, Y., & Li, Q. (2022). Seeking medical advice in mobile applications: How social cue design and privacy concerns influence trust and behavioral intention in impersonal patient–physician interactions. *Computers in Human Behavior*, *130*, 107178.