Human Interaction and Emerging Technologies (IHIET 2024), Vol. 157, 2024, 519–527
https://doi.org/10.54941/ahfe1005511

Privacy Policy Analysis and Evaluation of Mobile Psychological Consultation Services in Saudi Arabia

Abdulmajeed Alqhatani

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

ABSTRACT

Psychological consultation apps have been increasingly used in the last few years. These services collect a variety of sensitive personal information. Typically, a privacy policy is the main way to reduce users' concerns about sharing personal health information. However, psychological consultation apps are considered an emerging service and their privacy practices have not been fully explored. This study analyzes and evaluates the privacy policies and Terms of Service (ToS) agreements of four Saudi psychological consultation apps, focusing on seven key privacy practices: types of collected information, the purpose of data collection, data sharing, data ownership, data retention, data storage and protection, and notifications about policy and ToS updates. Overall, the findings indicate that the privacy policies of these services must be improved to better inform users, particularly regarding the purpose of collecting their data, with whom the data are shared, and what data are archived. This paper also provides a set of implications to improve the existing privacy policies of psychological health apps.

Keywords: Psychological health apps, Mental health apps, Privacy, Privacy policy, mHealth

INTRODUCTION

Mobile Health (mHealth) has become widely used, especially after the global COVID-19 pandemic. In Saudi Arabia, the use of mHealth services has increased Significantly (Alanzi, 2022), and this increase can also be attributed to the National Transformation Program which encourages rapid digitalization of healthcare services. Psychological consultation apps are an mHealth service that people find helpful. Such apps provide users with therapeutic and consultation services, including live sessions and instant messaging with psychotherapists, symptom tracking, and social support. Studies indicate that these health apps can positively impact users (Marques et al., 2021).

Given the nature of such services, users may need to disclose personal information to the application and the consultants, and some of this information can be considered sensitive. Typically, privacy policies and ToS agreements are the main mechanism to communicate to users how their personal information is collected, shared, and protected. Yet in terms of

mHealth, these services are still new, and their privacy practices have been relatively unexplored.

This study analyzes and compares the privacy policy of four popular Saudi apps that are used for psychological consultation, focusing on seven practices: types of information collected, the purpose of data collection, data sharing, data ownership, data retention, data storage & protection, and policy updates. This paper makes the following contributions:

- Analysis of the privacy polices of four popular Saudi Psychological health apps that collect sensitive personal information.
- Evaluation that reveals the privacy policies of psychological health apps lack sufficient details regarding key practices about which users should be informed.
- Identification of a set of design implications and future research opportunities to improve the privacy policies of this important type of mHealth services.

BACKGROUND

"The authors would like to indicate that the terms psychological health, psychological support, and mental health are used interchangeably throughout the remainder of the paper."

Psychological Health Applications

Mobile Health (mHealth) apps present new and convenient methods for personal health management. These digital technologies are perceived by health professionals to promote the wellbeing of users. Among mHealth apps that have gained attention are those used for tracking mental health issues, such as depression and anxiety (Linardon et al., 2024; Atallah et al., 2017). During and after the global coronavirus (COVID-19), The use of apps for tracking psychological health has especially become prevalent (Alanzi, 2022). Marques et al. (2021) studied the impact of Covid-19 on the mental health of Spanish university students, and the findings show that many of the participants were willing to use mobile apps to manage their mental health.

However, there are some issues that might hinder the use and engagement with health apps, such as usability and ease of use, lack of trust, and privacy issues (Alqahtani and Orji, 2020; Qingchuan Li, 2020). The study by Alqahtani and Orji (2020) analyzed user experience with mental health apps, and they found several factors that impact people to abandon the use of mental health applications; those factors include mainly poor usability security, privacy, and trust concerns. Privacy issues cannot be ignored given the sensitivity of some of the information collected about users of psychological health apps. Li (2020) indicates that privacy concerns may have a significant impact on the use of health applications. The next part of this section discusses privacy concerns related to medical apps, including psychological health apps.

Privacy Concerns

Medical applications collect a variety of personal data ranging from contact (e.g., phone number and email) to demographic (e.g., age and gender) and health-related information (e.g., biometrics). This collection can impose several privacy issues (Sharma et al., 2021; Lustgarten et al., 2020). For example, data breaches targeting digital healthcare systems can negatively impact its users, including embarrassment and reputation damage (Iwaya et al., 2020). There is also a concern that users' data inside those health apps might be shared with third parties without users' awareness (Kitkowska et al., 2023).

Researchers have further explored mHealth apps to understand users' behaviors and potential solutions to privacy problems. Building upon the privacy paradox, Zhu et al. (2021) indicate that users of mHealth are intended to disclose their personal information if they perceive benefits. However, people sharing preferences in health applications may also be affected by other factors, such as trust and previous security and privacy incidents (Kitkowska et al., 2023). Implementing social cue factors within health apps can decrease privacy concerns when users are interacting with both physicians and the application itself (Zhang et al., 2022).

To protect the sharing and use of personal data in digital systems, several governments have initiated regulations, such as the European Union's General Data Protection Regulation (GDPR) and the Saudi's Personal Data Protection Law (PDPL). Given the current advancements in digital systems, those regulations may not fully address the issue (Nurgalieva et al., 2020). A key privacy protection method is to improve users' awareness about service providers' data practices through privacy policies, which will be discussed next.

Privacy Policy

Privacy policy is a legal document presented by a service provider to explain the different practices in relation to users' data. For example, it specifies what data will be collected from a user and for what reasons, with whom it will be shared, and how it will be protected. However, psychological support apps can be considered new in the context of the mobile app industry, and privacy practices related to those apps have not been fully addressed.

Parker et al. (2019) analyzed 61 mental health apps from a dominant-English speaking market, and they found that nearly half of the examined apps did not provide a privacy policy for users. In a similar study, Robillard et al. (2019) reviewed 100 mental health apps from popular digital stores, indicating that most of the apps did not provide a privacy policy and a ToS agreement. Rowan & Dehlinger (2014) conducted a comparison study of the privacy policies of health and fitness tracking applications. Their study shows that specific permissions in those apps are insufficiently addressed by the privacy policy developers.

If people are to provide their mental health information, it is important to evaluate the transparency of the service's data practices. O'Loughin et al. (2019) evaluated the transparency of data processing in mobile apps used

for depression. Out of 116 apps examined in their study, only 4% of apps were assigned an "acceptable" score for transparency. Huckvale et al. (2019) evaluated the content of privacy policies of apps used for depression and smoking, and only 64% of those policies presented descriptions about secondary uses of the data. It is essential to inform users about sharing their personal information with external parties, as previous studies have demonstrated that mHealth data can be aggregated from multiple sources and re-identified (Galvin & Demuro, 2020). This current study differs from previous research in that it focuses on 7 key practices that a privacy policy should address to enhance users' awareness of sharing their mental health information.

METHODOLOGY

This research seeks to understand the data practices of mental health app companies by analyzing these apps' privacy policies. Figure 1 below shows the methodology applied for that analysis.

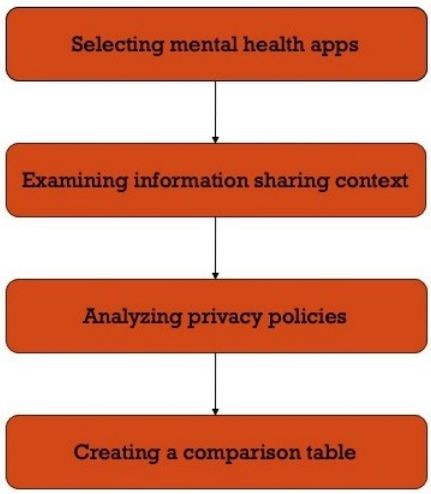

Figure 1: Study procedure.

The first phase involved identifying the selection criteria for choosing the apps to be examined. To be included in the study, each app had to satisfy two conditions: (a) it must be approved by the Saudi Ministry of Health, (b) and must have a release date in or prior to 2020. Using those inclusion criteria, the author searched the Apple App store for mental health apps using the key word "psychological consultation." Apps that satisfied the conditions were then selected based on the "top charts" feature in the Apple store. Four mental health-related apps were downloaded for analysis that were ranked among the top 100 "medical" and "health and fitness" apps in the Apple store, namely, Labayh, Estenarh, Tetaman, and Famcare.

In the second phase, the author signed up and used each service for a while in order to understand the possible situations and scenarios that require

sharing different personal information in each service. For example, some apps optionally request the disclosure of certain health information, such as asking about the mental health history of a user and the user's family or whether a customer has ever been harassed or bullied for the purpose of evaluating a case.

Next, three evaluators independently read and take notes of each app's privacy policy and ToS agreement, focusing on the seven primary data practices (previously mentioned in the introduction) that privacy policies normally address.

In the last phase, each service policy was summarized and a table was created to compare the commonalities and differences between these policies regarding of the seven evaluation criteria. The evaluators then discussed each policy together and an overall score was assigned to each service representing the extent to which the privacy policy fulfills each of those privacy aspects.

EVALUATION

In this section, each service privacy policy and ToS agreements are described in the light of the seven identified criteria for privacy. Then, a table that summarizes and rates each policy is presented to assess how well each of the privacy aspects is implemented in each service.

Analysis of Privacy Policies

Types of collected information. Companies, typically, collect different personal information from users to enable the provision of services or shape future improvements. Yet service providers must inform users about what personal information is being collected about them. Overall, each service seems to collect a variety of personal data, including gender, birth date, marital status, mobile number, email, medical history, and payment information. Labayh, Tetaman, and Famcare seemed to thoroughly identify the types of information they collect about users by classifying information into the following categories: basic account information (name, password, mobile number, payment information, information regarding customers' complaints, evaluations of consultants by customers, and information sent by users to company email addresses. However, Famcare privacy policy also states that they may collect users' information from other sources and aggregate it for analysis.

Purpose of information collection. One important aspect that impacts users' willingness to share their mental health information is whether they are informed about how their information will be used. Estenarh and Famcare provide detailed descriptions about the purpose of collecting personal data, such as using cookies and log data to provide technical services and use content for advertisements. However, in its policy, Estenarh mentioned that it may not require a user's consent to use some of the recorded data in the app. The other two apps did not provide an explicit statement in their policy describing why they collect users' information.

Data sharing. Users' comfort levels depend on who will have access to their personal information via data sharing (Galvin and DeMuro, 2020). Labayh

and Tetaman assert that users and consultants data will not be shared with any party other than what is permitted according to the law of Saudi Arabia, and that the data will only be accessible to the service team only. Famcare indicates that users' data will not be shared with external parties without users' consent. Estenarh mentioned that the recorded data may be shared with several parties, including the judicial authority, research parties, and future owners of the service.

Ownership of data. Use and sharing decisions can significantly be influenced by the level of control a user has over personal information. Estenarh states that users can be somewhat in control over their data through the account settings, but some data will still be kept even if users opt-out of the service. The other services did not clearly explain how users can be in control of their own personal data.

Data retention. One major concern of users when using a service, especially health-related services, is whether the service provider keeps the data after users stop using the app and, if so, for how long. Labyah and Tetaman policies include vague statements, indicating that users' data will be retained as long as the user continues to use the service and as long as the account remains registered in the service. Those statements are each followed by a statement indicating that some personal data will be retained for lawful and regulation reasons. Famcare mentioned in its policy that some basic user's information will be deleted from their servers if the user requests so, but other information will be saved as long as the Famcare needs it. Estenarh clearly identified a list of information that will be archived for commercial, technical, and lawful reasons.

Data storage & protection. The examined services provide about the same level of data security. Their policy states that users' data, such as passwords, will be encrypted. Estenarh privacy policy additionally states that any documents shared by a user will be encrypted and that the connection between the client and the consultant will completely be confidential.

Policy changes. All the services state that they will post any modifications to their privacy policies directly in the application. The ToS agreement of both Labyah and Tetaman and the privacy policy of Famcare state that users may also be notified via email about any amendment to the service and user conditions.

Comparison Table

Table 1 below summarizes the previous investigation of the privacy policy and ToS agreement of each app in terms of the seven privacy criteria. For each service, a score is assigned that shows how well each privacy aspect has been described in each policy (where: 0 = not described, 1 = partially described, and 2 = fully described). An overall score is also calculated for the privacy policy of each service.

Table 1. Evaluation of the Four Privacy Policies.

	Labyah	Estenarh	Tetaman	Famcare
Types of collected information	2	1	2	2
Purpose of information collection	0	1	0	2
Data sharing	1	2	1	2
Ownership of data	1	2	1	1
Data retention	1	2	1	1
Data storage & protection	1	2	1	1
Policy updates	2	1	2	2
Total score (out of 14)	**8**	**11**	**8**	**11**

IMPLICATIONS

Improving transparency - Studies indicate that users are willing to disclose their personal information for the sake of their wellbeing and mental health (Zhu et al., 2021). However, if users do not feel that they are in control of their personal information, they might give up using the service. Thus, privacy policymakers should provide clear and easily understandable descriptions of how users' information is handled by the app. When data is shared with external parties, users should have a choice to share their information in part or in full, and they should be allowed to opt-in and out at any time. Therefore, users will feel more comfortable about sharing their data and so will be able to build trust with the app.

Anonymization - Given the nature of psychological consultation apps, users are likely to disclose sensitive personal information to the consultant during treatment sessions or to the app itself. The disclosed information may contain personally identifiable information and is typically stored in the servers of the app's company. Previous incidents have shown that health information is valuable to hackers. In this study, only one service mentioned that users' information will be anonymized. If data breaches occur on a company's server, customers' information will be compromised. Therefore, mHealth apps should implement anonymization techniques, such as data masking and generalization to protect the confidentiality of customers' information.

Visual cues - One issue with a privacy policy is that it usually comes lengthy and full of jargon, which enforces users to skip reading it. Rather, visual cues can engage a user to pay attention to specific information in the privacy policy. Such cues can be as simple as different text colors to represent sensitive personal information collected by the app. It can also be designed as comics to summarize key information in the policy (Tabassum et al., 2018).

Compliance with regulations - The increasing advancements in digital technologies mean that regulations, such as the GDPR need to be reviewed and updated. This also means that mHealth companies need to ensure that their privacy policies align with existing regulations. Conducting regular assessments of a privacy policy and a ToS is a good practice to ensure compliance with existing laws and regulations.

LIMITATIONS

The present study has two limitations. First, it was limited to analyze the privacy policies of psychological consultation apps in the Saudi market. The reason for this decision is because Saudi Arabia has witnessed a significant growth in the development of mHealth apps, and we wanted to explore the current privacy practices by mobile app companies in this market. Second, the study investigates the policies of the top five mental health apps in the Apple App store only, which represents a small portion of apps for mental health.

CONCLUSION

Mental health apps are still emerging in the context of medical apps, and the privacy policies of these services have not been fully studied. With the goal of assessing the current-sate of transparency in the privacy practices of psychological consultation apps, this study analyzes four services that are approved by the Ministry of Health in Saudi Arabia. The overarching findings of this study indicate that the privacy policies lack transparency regarding why certain data are collected, with whom data are shared, and what data are retained after a user stops using the service. Further, while all services claim to protect users' data through encryption, only one service indicates that users' information will be anonymized if or when the app shares data with other parties. In the future, we plan to examine users' awareness and expectations about mental health app services and to what extent those expectations align with the existing privacy policies.

ACKNOWLEDGMENT

The author would like to thank Aseel Reshan and Maryam Jammah for helping in the analysis process.

REFERENCES

Alanzi, T. M., 2022. Users' satisfaction levels about mHealth applications in post-Covid-19 times in Saudi Arabia. *PloS one*, *17*(5), p. e0267002.

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

Atallah, N., Khalifa, M., El Metwally, A. and Househ, M., 2018. The prevalence and usage of mobile health applications among mental health patients in Saudi Arabia. *Computer methods and programs in biomedicine*, *156*, pp. 163–168.

Galvin, H. K. and DeMuro, P. R., 2020. Developments in privacy and data ownership in mobile health technologies, 2016–2019. *Yearbook of medical informatics*, *29*(01), pp. 032–043.

Huckvale, K., Torous, J. and Larsen, M. E., 2019. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open*, *2*(4), p. e192542.

Iwaya, L. H., Ahmad, A. and Babar, M. A., 2020. Security and privacy for mHealth and uHealth systems: A systematic mapping study. *IEEE Access*, *8*, pp. 150081–150112.

Kitkowska, A., Karegar, F. and Wästlund, E., 2023, September. Share or Protect: Understanding the Interplay of Trust, Privacy Concerns, and Data Sharing Purposes in Health and Well-Being Apps. In *Proceedings of the 15th Biannual Conference of the Italian SIGCHI Chapter* (pp. 1–14).

Li, Q., 2020. Healthcare at your fingertips: The acceptance and adoption of mobile medical treatment services among Chinese users. *International journal of environmental research and public health*, *17*(18), p. 6895.

Linardon, J., Torous, J., Firth, J., Cuijpers, P., Messer, M. and Fuller-Tyszkiewicz, M., 2024. Current evidence on the efficacy of mental health smartphone apps for symptoms of depression and anxiety. A meta-analysis of 176 randomized controlled trials. *World Psychiatry*, *23*(1), pp. 139–149.

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T. and Flynn, A. W., 2020. Digital privacy in mental healthcare: Current issues and recommendations for technology use. *Current opinion in psychology*, *36*, pp. 25–31.

Marques, G., Drissi, N., de la Torre Díez, I., de Abajo, B. S. and Ouhbi, S., 2021. Impact of COVID-19 on the psychological health of university students in Spain and their attitudes toward Mobile mental health solutions. *International Journal of Medical Informatics*, *147*, p. 104369.

Nurgalieva, L., O'Callaghan, D. and Doherty, G., 2020. Security and privacy of mHealth applications: a scoping review. *IEEE Access*, *8*, pp. 104247–104268.

O'Loughlin, K., Neary, M., Adkins, E. C. and Schueller, S. M., 2019. Reviewing the data security and privacy policies of mobile apps for depression. *Internet interventions*, *15*, pp. 110–115.

Parker, L., Halter, V., Karliychuk, T. and Grundy, Q., 2019. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International journal of law and psychiatry*, *64*, pp. 198–204.

Robillard, J. M., Feng, T. L., Sporn, A. B., Lai, J. A., Lo, C., Ta, M. and Nadler, R., 2019. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet interventions*, *17*, p. 100243.

Rowan, M. and Dehlinger, J., 2014. A privacy policy comparison of health and fitness related mobile applications. *Procedia Computer Science*, *37*, pp. 348–355.

Sharma, T., Islam, M. M., Das, A., Haque, S. T. and Ahmed, S. I., 2021, June. Privacy during pandemic: A global view of privacy practices around COVID-19 apps. In *Proceedings of the 4th ACM SIGCAS Conference on Computing and Sustainable Societies* (pp. 215–229).

Tabassum, M., Alqhatani, A., Aldossari, M. and 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).

Zhang, J., Luximon, Y. and 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*, p. 107178.

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X. and Yuan, Q., 2021. Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, *61*, p. 101601.