Advanced Research on Information Systems Security

ARIS²
an international journal

ISSN: 2795-4609 | ISSN: 2795-4560

Print & Online

Ethical and legal aspects of cybersecurity in health: mental health monitoring and management applications

Ana Galvão [a*], Clara Vaz [b], Marco Pinheiro [c], Clarisse Pais [d]

[a]*Polytechnic Institute of Bragança – UICISA:E, Campus de Santa Apolónia, 5300-253 Bragança, Portugal*

[b]*Polytechnic Institute of Bragança – Research Centre in Digitalization and Intelligent Robotics (CeDRI), Campus de Santa Apolónia, 5300-253 Bragança, Portugal*

[c]*Iscte – Instituto Universitário de Lisboa, Avenida das Forças Armadas, 1649-026 Lisboa, Portugal*

[d]*Polytechnic Institute of Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal*

[a]*Email: anagalvao@ipb.pt*

[b]*Email: clvaz@ipb.pt*

[c]*Email: marco.paulo.pinheiro@iscte-iul.pt*

[d]*Email: clarisse@ipb.pt*

Abstract

Background: With the emergence of eHealth and mHealth, the use of mental health apps has increased significantly as an accessible and convenient approach as an adjunct to promoting well-being and mental health. There are several apps available that can assist with mental health monitoring and management, each with specific

features to meet different needs. The intersection of mental health and cyber technology presents a number of critical legal and ethical issues. As mental health monitoring apps and devices become more integrated into clinical practice, cybersecurity takes on paramount importance. Objective: To address the ethical and legal aspects of health cybersecurity related to applications in mental health monitoring and management. Methods: We carried out a thematic synthesis of the best scientific evidence. Results: These tools have the potential to significantly improve access to and quality of care for users with mental health conditions, but they also raise substantial concerns about privacy and informed consent. Cybersecurity in mental health is not only a matter of technology, but also of human rights. The protection of sensitive mental health information is critical, and legal and ethical measures to safeguard this information must be implemented in a robust and transparent manner. Conclusion: the use of information technologies and mobile devices is now part of the clinical reality and its future perspectives. It is important to mention that while these apps can be helpful for self-care and mental well-being management, they are not a substitute for the advice and support of a qualified mental health professional (psychologist or psychiatrist). As we move into the digital age, it is imperative that mental health monitoring and management apps are developed and used responsibly, ensuring the safety, dignity, and well-being of users.

Keywords: ethics; cybersecurity; mental health applications; legal aspects

Citation: A. Galvão, C. Vaz, M. Pinheiro, and C. Pais, "Ethical and legal aspects of cybersecurity in health: Mental health monitoring and management applications", ARIS2-Journal, vol. 4, no. 1, pp. 04–19, Apr. 2024.

DOI: https://doi.org/10.56394/aris2.v4i1.45

---

* Corresponding author. Email address: anagalvao@ipb.pt

1. Introduction

Technology has brought significant advances in the promotion of mental health, with the emergence of apps and online platforms that help and accompany users in their day-to-day lives. Apps and online platforms offer users convenient access to tools that can help with self-monitoring and management of stress, anxiety, and other psychological disorders. Although they do not replace traditional therapy and follow-up by properly trained professionals, these tools are used to promote mental health and emotional well-being.

We know that 29% of the population experiences psychological health problems at some point in their lives. One in four people live with psychological health problems. Although these difficulties and psychological health problems are frequent, most people with psychological health problems are unable to access the mental health

services they need [1].

As a general objective of the chapter, we propose to reflect on the ethical and legal aspects of cybersecurity in the use of applications in the monitoring and management of mental health.

1.1. Background

In the evidence consulted, we identified the following as positive aspects related to the use of applications in the monitoring and management of mental health.

Convenient Access:

- 24/7 availability: Applications provide ongoing support, allowing users to access resources anytime, anywhere.
- Reduced Geographic Barrier: Eliminate geographic barriers, providing access to mental health services for people in remote areas or who have difficulty accessing traditional services.

Variety of Features:

- Self-monitoring and self-management of symptoms: some apps allow the user to fill in validated scales that provide them with the level of anxiety, stress and personality traits;
- Meditation and Relaxation: Many apps offer meditation, relaxation, and breathing exercises to help reduce stress and anxiety.
- Mood Tracking: Some apps allow users to monitor their mood over time, identifying patterns and sharing data with mental health professionals if desired.
- Self-care: some apps highlight the importance of food in mental health, as well as the practice of physical activities that promote mental health and general well-being.

Customization and Personalization:

- Personalized Treatment Plans: Some apps offer personalized treatment plans based on the user's individual needs and goals.
- Personalized Feedback: They provide personalized feedback based on user interactions and progress.

Confidentiality and Privacy:

- Protected Confidentiality: The best apps ensure the protection of the privacy and confidentiality of user data

by following strict security practices.

- Anonymous Options: Some apps offer the option of anonymous use for those who want more privacy.

Integration with Traditional Therapy:

- Complement to Therapy Services: These can be used as a complement to traditional therapy services, allowing users to practice skills learned between sessions.
- Reports for Professionals: Some apps allow users to share reports or information with their mental health professionals.

Education and Awareness:

- Educational Resources: Offer psychoeducational information about mental health, specific disorders, and coping strategies.
- Awareness: Contribute to awareness and reduction of stigma related to mental health.

Cost and Accessibility:

- Affordable or Free Cost: Many apps offer free basic versions or come at an affordable cost compared to traditional mental health services.
- Democratization of Access: They contribute to the democratization of access to mental health care, making it more accessible to a variety of people.

Progress Tracking:

- Progress Logging: Allows users to track their progress over time, encouraging consistency and practice of self-care techniques.

Crisis Support:

- Emergency Resources: Some apps include crisis support features, such as emergency services hotlines and contact information.

Despite the benefits listed, it is important to recognize that the apps are not a substitute for guidance from mental health professionals. Choosing an app should be made with caution, considering quality, safety, and suitability for individual needs. Additionally, in more severe cases, it is essential to seek professional help.

1.2. Ethical and cybersecurity issues

Despite the significant benefits, there are also ethical and cybersecurity issues that need to be considered. Some of the main ethical concerns associated with the use of apps in the area of mental health:

Privacy and Confidentiality:

- Sensitive Data Harvesting: Many mental health apps collect personal and sensitive data. It is crucial to ensure the privacy and confidentiality of this information. Regulations such as the European Union's General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) set stringent standards for handling health information. Mental health apps must ensure data encryption and implement safeguards against unauthorized access.
- Informed Consent is a crucial ethical aspect: Users must be clearly informed about the type of data being collected, how it will be used and shared. This includes understanding the potential risks associated with cybersecurity, such as the possibility of a data breach. Apps should provide clear and accessible terms to ensure that users can make informed choices.

Cybersecurity:

- Protection Against Attacks: Ensure robust cybersecurity measures are in place to protect data from threats such as hacker attacks and information leakage.

Quality and Accuracy of Information:

- Clinical Effectiveness: The accuracy of the information provided by the apps and the clinical effectiveness of their interventions must be supported by solid scientific evidence.

Equity in Access:

- Equity in access is an important ethical concern, particularly in contexts where technology is proposed as a solution to gaps in mental health service delivery. Careful consideration should be given to ensuring that such tools do not exclude individuals based on geographic location, socioeconomic status, or ability to use technology.

Transparency and Accountability:

- Transparency in Practices: App developers and vendors must be transparent about their practices, including decision-making algorithms and recommendation processes.
- Accountability: Establish accountability for application failures or for unexpected consequences of use,

ensuring that there is a clear solution to resolve issues.

Artificial Intelligence and Decision Making:

- Algorithmic Biases: Applications that use artificial intelligence for data analysis may exhibit biases. It is necessary to monitor and mitigate these biases to ensure fairness and equity.

Consent of Minors:

- Parental Consent: In the case of apps intended for minors, obtaining parental consent is essential, as well as ensuring that the information is presented in a way that is appropriate for understanding the age.

Appropriate Therapeutic Relationship:

- Replacement *vs*. Add-on: Clarify whether the app is intended to replace or complement traditional and therapeutic treatments. Complete replacement may raise ethical concerns.

Feedback and Human Intervention:

- Limitations of Apps: Recognize the limitations of apps in the delivery of mental health care and ensure that there is the possibility of human intervention when needed.

Continuous Evaluation and Ethical Update:

- Ethical Monitoring: Conduct regular ethical assessments as apps evolve, ensuring that they continue to adhere to ethical standards and respect users' rights. Continuous training in cyber ethics and information security should be a priority for the professionals involved.

When developing, implementing, or using mental health apps, it is crucial to consider these ethical issues to ensure that the benefit to the user is maximized while minimizing potential risks. By addressing both ethical and legal aspects, mental health app developers and service providers can build a strong foundation for delivering safe, ethical, and effective services. Collaboration with ethics, privacy, and cybersecurity professionals is essential to ensure compliance and the integrity of the service offered.

2. Materials and methods

Given its standardization, the preparation of an integrative review presupposes rigor and transparency. To carry out this study, we followed guidelines. Similarly, the writing of this chapter was organized to meet the PRISMA-

ScR checklist, developed by for reporting integrative reviews. According to, the recommended steps for conducting an integrative review are: (1) to identify the research question(s); (2) to search for relevant studies; (3) to select the studies; (4) to analyze the results; and (5) to group, summarize and present the results [2], [3], [4].

The conduct of this integrative review aimed to answer the following research question: What are the ethical and cybersecurity issues present in the use of Mental Health apps?

2.1. Search for Relevant Studies

Prior to the identification of potentially relevant studies, the search terms were determined in line with the research question and organized according to the SPIDER model, an acronym for Sample, Phenomenon of Interest, Design, Evaluation and Research. In this study, the search was conducted in the Web of Science Core Collection and Scopus databases, using the following search terms, Boolean operators and inclusion criteria: [5]

- S: “mental health app*”
- PI: ("legal aspects" OR "legal requirements" OR "ethic* issues" OR "ethic* requirements" OR "patient privacy" OR "consent" OR "data governance" OR "data protection" OR "data security" OR “security”)
- D: any
- E: There are
- R: (“quantitative” OR “qualitative” OR “mixed”)

Resulting in the following total search key: "mental health app*" AND ("legal aspects" OR "legal requirements" OR "ethic* issues" OR "ethic* requirements" OR "patient privacy" OR "consent" OR "data governance" OR "data protection" OR "data security" OR “security”)

Besides the search terms, the following filters were applied:

- Years included: all
- Type of access: open access
- Type of documents: articles and publications in scientific congress proceedings
- Type of studies: all, except revisions
- Languages: documents in English, Portuguese, Spanish, French and German

Data extraction was performed in January 2024.

The evidence searches and selection process is summarized in a flowchart, according to PRISMA-ScR (Figure 1).

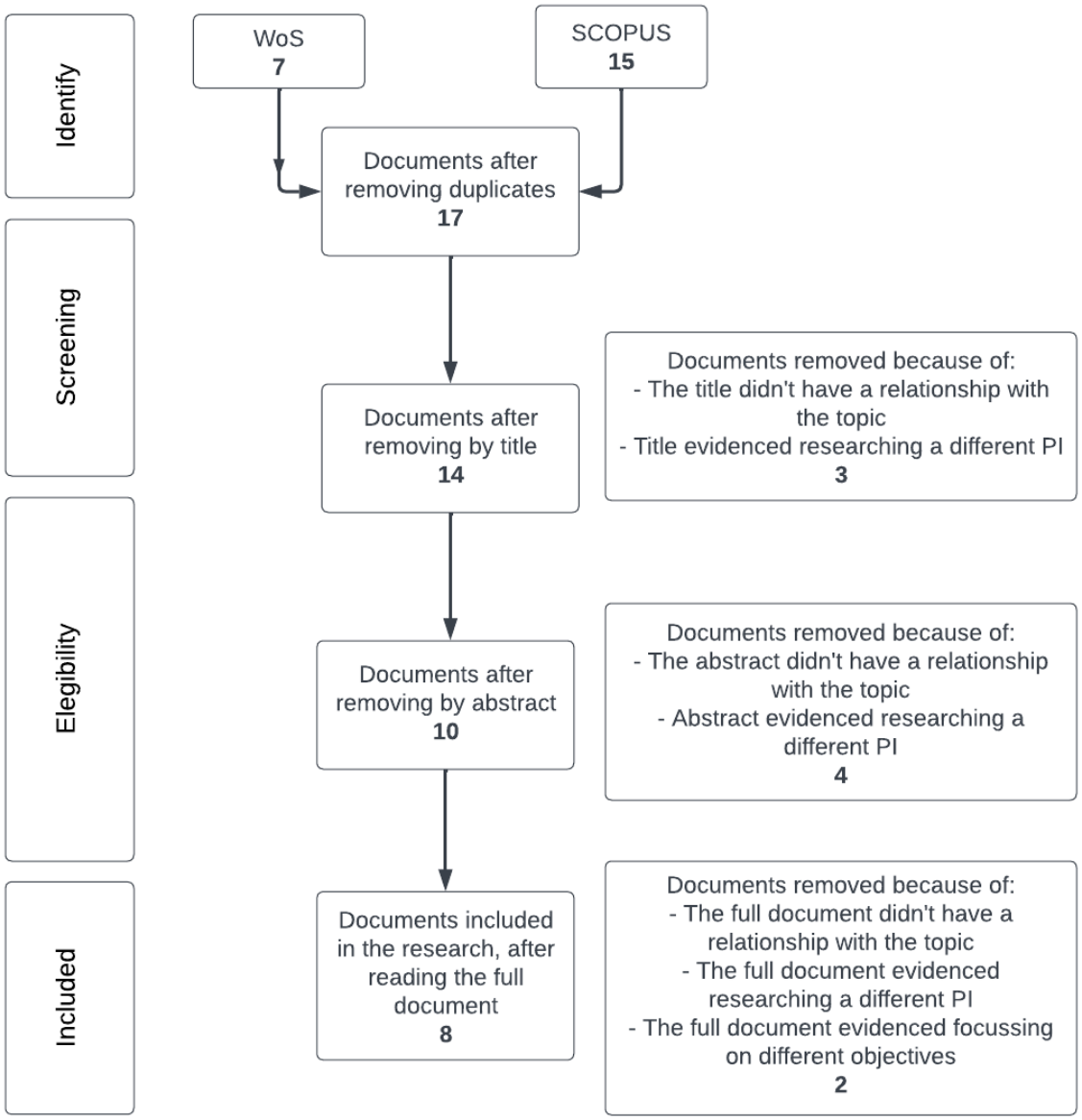

Figure 1: Document selection flowchart

2.2. Analysis of Results

The analysis of the title, abstract and full text was always performed by two or more independent researchers of the research team, who selected the articles to be considered for review based on the inclusion and exclusion

criteria. Data extraction was performed by three of the researchers, basing the instrument developed around the objectives and research questions, defined for the study, on the Joanna Briggs Institute model [6].

2.3. Presentation of the Results

The research findings were organized according to the SPIDER model, an acronym for Sample, Phenomenon of Interest, Design, Evaluation and Research type and summarize the results in an organized and easily interpretable table [5].

3. Results

We present the results of our research organized according to the SPIDER methodology (Table 3), where it becomes evident that most mental health applications lack security, clear privacy rules and a low digital literacy of the end-users.

Table 1 - Organization of selected documents, according to the SPIDER methodology

Authors and year	Sample	Phenomenon of interest	Design	Evaluation	Research type
[7]	105 mental health app users	Investigate the security awareness of mobile health app users	Simulation of some common security attack scenarios in the context of mHealth	A minority of our participants perceived access permissions positively, the majority had negative opinions. Users provide their consent by granting permissions, without careful review of privacy policies that leads to unwanted or malicious access to health data. The results also indicated that 73.3% of our participants denied at least one access permission, and 36% of our participants preferred no authentication method.	Quantitative
[8]	101 mental health app users	Investigate security awareness of (i) existing and desired security features, (ii) security-related issues, and (iii) methods to improve security knowledge.	End-user survey-driven case study in collaboration with two mHealth providers in Saudi Arabia	The results indicate that while security awareness among different demographic groups was statistically significant based on their level of IT knowledge and level of education, security awareness based on gender, age, and frequency of use of the mHealth app was not statistically significant. The jury also found that the majority of end-users are unaware of the existing security features provided (e.g. restricted permissions	Qualitative

Authors and year	Sample	Phenomenon of interest	Design	Evaluation	Research type
				for applications); However, they want usable security (e.g., biometric authentication) and are concerned about the privacy of their health information (e.g., data anonymization). End users have suggested that protocols such as two-factor authentication positively affect security but compromise usability.	
[9]	27 Mental Health Apps	Systematically identify and understand data privacy embedded in mental health apps	Conduct in-depth analysis of application privacy, covering static and dynamic analysis, data sharing behavior, server-side testing, privacy impact assessment requests, and privacy policy evaluation. In addition, we mapped the findings to the LINDDUN threat taxonomy, describing how threats manifest in the applications studied.	The findings reveal important data privacy issues, such as unnecessary permissions, insecure encryption implementations, and leaks of personal data and credentials in logs and web requests. There is also a high risk of user profiling, as application development does not provide foolproof mechanisms against linking, discoverability, and identifiability. The sharing of data between third parties and advertisers in today's app ecosystem exacerbates this situation.	Quantitative

Authors and year	Sample	Phenomenon of interest	Design	Evaluation	Research type
[10]	98 Mental Health Apps	Systematically evaluate features, functionality, data security, and congruence with evidence of self-guided CBT-based apps targeting users affected by depression that are available in major app stores.	Reports through a narrative review using descriptive statistics.	While most apps included a privacy policy, only a third of apps had one before the account was created. In total, 82% (74/90) of privacy policies stated that they share data with third-party service providers.	Quantitative
[11]	104 specialists, 80 students and 85 patients	Explore the attitudes, expectations, and concerns of medical experts, including physicians, psychotherapists and nursing staff, medical or psychology students,	The measures focused on existing knowledge and experience with online mental health applications, followed by a question on whether the development of e-health was generally accepted or disliked. In addition, we asked about	All groups reported slight concerns regarding data security (mean 0.85, SD 1.09; 95% CI 0.72-0.98)	Quantitative

Authors and year	Sample	Phenomenon of interest	Design	Evaluation	Research type
		and patients regarding e-mental health apps when considering their previous knowledge and experience with e-mental health apps	the expectations for an ideal mental health app and possible concerns felt by the participants. All items were presented on a 5-point Likert scale or as multiple-choice questions. In addition, 4 items were presented as open text fields.		
[12]	18 Mental Health Apps	Verify GDPR compliance	Analysis of security standards and organization of descriptive data	78% do not provide any information on how personal data is processed, and if they do, this is unclear. In addition, users' consent is rarely sought to allow such processing (11%).	Quantitative
[13]	61 Mental Health Apps	Identify salient privacy-related consumer issues in the mental health app market and inform advocacy efforts to	Critical content analysis of promotional (advertising) materials for prominent mental health apps in selected dominant English-speaking	Nearly half of apps (25/61, 41%) did not have a privacy policy to inform users about how and when personal information would be collected and retained or shared with third parties, despite this being a standard recommendation of privacy regulations.	Quantitative

Authors and year	Sample	Phenomenon of interest	Design	Evaluation	Research type
		advance consumer interests	markets in late 2016 and early 2017, updated in 2018.		
[14]	50 Mental Health Apps	Explore potential ethical, data security, and privacy issues associated with the use of Mental Health apps for depression	Cross-sectional evaluation of the top 50 MH apps (in order of Google Play Store search results) for depression available in India was conducted in November 2021.	The majority of apps were listed in the health and fitness category (54%). The median number of total and dangerous permissions requested at the time of download was nine and three, respectively. The English privacy policy was available to 76%. The average length of the privacy policy was 2171 words, and Flesch-Kincaid's average reading level was 12 (well above the recommended cut-off point of eight). Important features relevant to safeguarding consumer confidentiality, including names of third parties with whom user data could be shared (42%), explicit consent before sharing data with third parties (16%), and assurance regarding the collection of non-identifiable data (11%), were absent from most privacy policies	Quantitative

4. Discussion

M-Health has gained particular relevance in recent years, with more and more people accessing mobile devices and using its apps. The World Health Organization points to M-Health as a potential solution to the difficulties of accessibility to Psychological Health services and as a way to promote self-care, Psychological Health care and Health research. The aids of new technologies support better decision-making, emotional regulation, or interpersonal interactions. We found evidence of the potential of mental health apps as a low-intensity individual psychological intervention for people with mild or moderate signs of psychological health problems.

However, the results from our research show that most mental health applications do not comply with legal regulations about data privacy [10], [12], [13], [14], that those data privacy data are difficult to understand and normally only exist in English [7], [8], [11], and that users have concerns about security issues, which are justified, as most mental health applications show present security risks [8], [9].

5. References

[1] Ordem dos Psicólogos Portugueses, *Análise Crítica OPP - Utilização de Apps de Saúde Mental*. Lisboa, 2022.

[2] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *International Journal of Social Research Methodology: Theory and Practice*, vol. 8, no. 1, pp. 19–32, 2005, doi: 10.1080/1364557032000119616.

[3] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *The BMJ*, vol. 372, no. 71, pp. 1–9, 2021, doi: 10.1136/bmj.n71.

[4] H. Noble and J. Smith, "Reviewing the literature: Choosing a review design," *Evid Based Nurs*, vol. 21, no. 2, pp. 39–41, 2018, doi: 10.1136/eb-2018-102895.

[5] A. Cooke, D. Smith, and A. Booth, "Beyond PICO: the SPIDER tool for qualitative evidence synthesis," *Qual Health Res*, vol. 22, no. 10, pp. 1435–1443, 2012, doi: 10.1177/1049732312452938.

[6] Z. Jordan, C. Lockwood, Z. Munn, and E. Aromataris, "The updated Joanna Briggs Institute Model of Evidence-Based Healthcare," *Int J Evid Based Healthc*, vol. 17, no. 1, pp. 58–71, 2019, doi: 10.1097/XEB.0000000000000155.

[7] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "An empirical study on secure usage of mobile health apps: The attack simulation approach," *Inf Softw Technol*, vol. 163, 2023, doi: 10.1016/j.infsof.2023.107285.

[8] B. Aljedaani, A. Ahmad, M. Zahedi, and A. M. Babar, "End-Users' Knowledge and Perception about Security of Mobile Health Apps: An Empirical Study," *Journal of Systems and Software*, no. c, 2021, [Online]. Available: https://www.ponemon.org/

[9] L. H. Iwaya, M. A. Babar, A. Rashid, and C. Wijayarathna, "On the privacy of mental health apps: An empirical investigation and its implications for app development," *Empir Softw Eng*, vol. 28, no. 1, 2023, doi: 10.1007/s10664-022-10236-0.

[10] L. Martinengo *et al.*, "Self-guided cognitive behavioral therapy apps for depression: Systematic assessment of features, functionality, and congruence with evidence," *J Med Internet Res*, vol. 23, no. 7, 2021, doi: 10.2196/27619.

[11] G. Mayer, N. Gronewold, S. Alvarez, B. Bruns, T. Hilbel, and J. H. Schultz, "Acceptance and expectations of medical experts, students, and patients toward electronic mental health apps: Cross-sectional quantitative and qualitative survey study," *JMIR Ment Health*, vol. 6, no. 11, 2019, doi: 10.2196/14018.

[12] J. Muchagata and A. Ferreira, "Mobile apps for people with dementia: Are they compliant with the general data protection regulation (GDPR)?," *HEALTHINF 2019 - 12th International Conference on Health Informatics, Proceedings; Part of 12th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2019*, no. Biostec, pp. 68–77, 2019, doi: 10.5220/0007352200680077.

[13] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices," *Int J Law Psychiatry*, vol. 64, no. April, pp. 198–204, 2019, doi: 10.1016/j.ijlp.2019.04.002.

[14] S. Singh, P. Sharma, P. Ghimire, R. Shrestha, and S. Gnanavel, "Assessment of App Store Description and Privacy Policy to Explore Ethical and Safety Concerns Associated with the Use of Mental Health Apps for Depression," *Indian J Psychol Med*, vol. 45, no. 2, pp. 173–178, 2023, doi: 10.1177/02537176221142046.