Unveiling Privacy Measures in Mental Health Applications

MUHAMMAD HASSAN, University of Illinois Urbana-Champaign, USA
MASOODA BASHIR, University of Illinois Urbana-Champaign, USA

Mental health conditions have become a global public health issue, especially in the context of the COVID-19 pandemic. To cope with the increasing demand for mental health services, many people have turned to smartphone applications that offer various mental health solutions, such as therapy, counseling, and self-help. However, these applications also pose significant privacy risks for their users, as they collect and share sensitive personal and health information with third parties, often without adequate consent or transparency. In this study, we examine the privacy policies of popular mental health smartphone applications using the Fair Information Practice Principles (FIPPs), a widely recognized privacy framework. Our objective is to assess the extent to which these applications adhere to the FIPPs guidelines and to identify the gaps and challenges in their privacy practices. We hope that our findings can inform and guide policy makers and application developers to design more user-centric and robust privacy policies that ensure the safety and security of users' information.

CCS Concepts: • **Social and professional topics** → **Privacy policies**; • **Security and privacy** → *Privacy protections*;

Additional Key Words and Phrases: Privacy Policies; Mental Health Application; Policy Analysis

ACM Reference Format:
Muhammad Hassan and Masooda Bashir. 2023. Unveiling Privacy Measures in Mental Health Applications. In *Adjunct Proceedings of the 2023 ACM International Joint Conference on Pervasive and Ubiquitous Computing & the 2023 ACM International Symposium on Wearable Computing (UbiComp/ISWC '23 Adjunct), October 8–12, 2023, Cancun, Quintana Roo, Mexico.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3594739.3612879

1 INTRODUCTION

The prevalence of mental health conditions has risen in the United States in recent years, affecting a significant portion of the adult population. In 2021, the prevalence of mental illnesses among adults aged 18 or older was 22.8%, equivalent to 57.8 million Americans, up from 17.7% (39.8 million Americans) in 2008 ([4]). Alarmingly, among this population, 53.8% (31.3 million) perceived an unmet need for mental health services. Affordability was identified as the most common barrier to access mental health services, followed by mental health stigma, and provider shortages or wait time. These trends have been further exacerbated by the COVID-19 pandemic, with prolonged periods of social isolation identified as a leading cause of mental health issues. Fear of death, financial worries, and grief after bereavement have also been significant triggers for mental health stress factors in the wake of the pandemic[1]. This situation is a cause for great concern, as it has been observed worldwide and has affected people from all walks of life. Consequently, there is an urgent need for research into effective strategies to support individuals struggling with mental health issues.

The increasing prevalence of mental health issues has spurred the development of technological solutions, with mental health smartphone applications emerging as a prominent means of delivering mental health support. These applications offer a range of services, including self-management, cognition improvement, skills training, social support,

Manuscript submitted to ACM

symptom tracking, and journaling, and have the potential to assist individuals experiencing mental health challenges. In contrast to traditional mental health solutions such as psychotherapy, medication, hospitalization, and support groups, mental health smartphone applications can provide numerous benefits, such as increased accessibility, convenience, and cost-effectiveness, thereby potentially reducing barriers to access for users who may face challenges such as geographical distance and stigma [3] [25]. Moreover, health applications can offer continuous and real-time support and feedback, facilitate self-monitoring and self-regulation, and enhance engagement and adherence to treatment, thereby potentially improving treatment outcomes [21]. The use of data analytics and artificial intelligence can further augment the delivery of mental health care through personalization and optimization of care [19]. Therefore, mental health smartphone applications represent a promising solution to the growing problem of mental health issues, offering several advantages over traditional treatment methodologies, with the potential to improve the mental well-being of individuals who may otherwise face barriers to accessing or receiving treatment[9].

Mental health smartphone applications have the potential to transform the mental health industry by providing convenience and accessibility, but they also pose serious privacy risks for the users' Personally Identifiable Information (PII) and Personal Health Information (PHI). These applications collect sensitive and personal PII related to one's mental health, which could result in severe privacy breaches if not adequately protected. For example, a recent study by Mozilla found that top mental health applications lacked effective privacy mechanisms, exposing users to potential harms [12]. Another study by Tahaei et al. examined the privacy posts of health applications on StackOverflow, an online platform where programmers can ask and answer questions related to coding, revealing that unclear documentation by app marketplace and third-party libraries also hindered application developers' efforts to ensure proper data protection and privacy for health applications [28]. These privacy breaches not only violate user privacy rights but also deter them from using these applications, as a prior study indicated that privacy violation may reduce the willingness to install apps[30].

The use of mental health smartphone applications poses a significant risk to user privacy, as these applications require sensitive personal and health information (PII & PHI), leaving users vulnerable to potential privacy harms. Despite the sensitivity of the data, many of these applications lack adequate privacy protections and practices, which exacerbates the situation [15]. Furthermore, users have limited legal protection under the Health Insurance Portability and Accountability Act (HIPAA) when it comes to digital data, as most of these applications are not covered by the law [17]. The US Department of Health & Human Services (HHS) notes that health applications are not covered by the law unless they are provided or contracted by a HIPAA-covered entity, such as a healthcare provider or a health plan [2]. This raises concerns about the transparency of application developers and policymakers in ensuring the privacy of users is protected. Given these privacy risks, it is crucial to investigate and study the privacy policies that are put in place by the mental health application to promote transparency about data protection and safeguarding the privacy of mental health smartphone applications.

The primary aim of this study is to investigate the privacy ecosystem of mental health smartphone applications by analyzing their privacy policies. Specifically, we intend to examine the level of transparency on how user PHI and PII data is protected, as well as the measures that these privacy policies claim to enforce. Additionally, we aim to evaluate the performance of these privacy policies against standard privacy-preserving frameworks. Overall, this study intends to raise awareness about the data protection standards of mental health smartphone applications, with particular emphasis on the importance of transparency about user involvement and consent in the collection and processing of sensitive PII and PHI information. Our findings could provide valuable insight for policymakers and application developers to implement robust data protection practices and ensure the privacy of mental health applications users.

2 BACKGROUND

The use of mental health smartphone applications has grown significantly in recent years, offering various benefits to their users [5]. However, the collection of sensitive personal identifiable information (PII) and protected health information (PHI) has led to concerns regarding user privacy. Although the Health Insurance Portability and Accountability Act (HIPAA) provides legal protections for sensitive health data, many mental health applications fall outside the scope of HIPAA regulations. To address these concerns, mental health applications are expected to adopt privacy-preserving frameworks, such as the Fair Information Practice Principles (FIPPs), to ensure appropriate handling of personal information in their policies.

In the following section, we will review relevant literature regarding mental health applications, HIPAA, and FIPPs to provide a comprehensive understanding of the current state of privacy protection in mental health applications.

2.1 Mental Health Applications

The historical development of mental health solutions can be traced to the origins of psychology and psychiatry as scientific disciplines. Scholars have long promoted a holistic and preventative approach to mental health issues, which involves analyzing an individual's personal history, social context, and environmental factors, along with their mental conditions [22]. However, throughout most of the 20th century, mental health care was primarily dominated by the biomedical model that focused on diagnosis and treatment of conditions using medication and psychotherapy.

Technology solutions in the form of smartphone applications have become ubiquitous for our daily needs due to the proliferation of smartphones [7, 27]. Similarly, mental health applications are also becoming increasingly prevalent, aiming to provide self-help, education, prevention, or treatment for various mental health issues. These smartphone applications offer accessibility, affordability, interactivity, and user engagement. Additionally, they provide features such as gamification, feedback, reminder, self-diagnosis, journaling and tracking, and artificial intelligence [14, 24]. Nonetheless, these mental health applications are still evolving and facing challenges. Although these applications potentially improve the quality of mental health treatment for users due to their effective scalability, user-experience, engagement, and personalization, they also pose privacy risks, such as PII and PHI data harvesting, and sensitive data being shared with third parties [18].

2.2 Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law that sets standards for the protection and sharing of health information by health care providers, and health plans. HIPAA gives patients their rights to access and control their own health information [11]. HIPAA applies to physical health information as well as mental health information. It recognizes that mental health information may be more sensitive in nature and requires additional safeguards. For example, HIPAA requires patients to authorization to disclose psychotherapy notes, which are often recorded during private or group counseling sessions by mental healthcare professionals [11].

Despite the regulatory measures imposed by HIPAA, many mental health applications may not fall under the purview of HIPAA due to their development and offering by entities that do not qualify as covered entities or business associates. A patient using a mental health application to enter their own PHI, without any involvement of their health care provider or health plan, may be subject to fewer privacy protections as the application may not be obligated to comply with HIPAA regulations. This highlights the need for a robust and consistent framework to ensure privacy and data protection for users of mental health applications [10, 11].

2.3 Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) were first introduced in 1973 in a report by the Department of Health, Education, and Welfare Advisory Committee [13]. These principles serve as a set of privacy-preserving and data protection guidelines that have continued to be relevant and influential despite not being part of any official privacy regulation or law [8]. FIPPs have played a pivotal role in the development of other popular data security and privacy frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

FIPPs are essential in shaping how companies and governments approach privacy and user data protection. They provide a framework for evaluating the effectiveness of information systems and programs that affect individuals' privacy. In the context of mental health applications that fall outside the scope of HIPAA, FIPPs can be applied to ensure that user data is collected, processed, transported, and used in a transparent and fair manner, establishing FIPPs as a useful privacy-preserving framework [15]. *In the following, we will define each principle from FIPPs in context of mental health applications.*

(1) **Right of Access and Rectification**: The right of access and rectification in FIPPs stipulates that individuals should have the ability to access and review their personal information (PII and PHI) that a mental health app collects and processes about them and to request corrections or deletions of any inaccurate, incomplete, or outdated user data. It aims to empower users to ensure the quality, accuracy, and relevance of the functionality and services of MHA based off their collected PII and PHI. It also enables user autonomy, where users can review their data and make informed decisions about their consent to share and process their PII and PHI with MHA.
(2) **Accountability**: The Principle of Accountability entails that the mental health applications that collect and process such data should demonstrate their adherence to the relevant data protections, security regulations and policies. This involves establishing clear and transparent policies that define the roles and responsibilities of the internal and external individuals, including company employee and third parties who have access to the users' personal and health information, as well as providing adequate training to them on how to handle such information ethically. Moreover, accountability requires that the applications should regularly monitor and audit their compliance with their own policies.
(3) **Authority**: Principle of Authority relates to the safety of sensitive personal and health information (PII and PHI), which requires that only individuals with the appropriate authority and training should be able to access and process such information. The principle of authority further demands that the applications should clearly disclose in their policies who are the authorized individuals and entities that have access to and control over the users' mental health data. This ensures that the users' data is not misused or abused by unauthorized actors, further enhancing their transparency and trustworthiness.
(4) **Minimization**: The principle of Minimization requires that the applications that collect and process personal information should limit their data practices to what is necessary and relevant to achieve a legally authorized purpose. This implies that the applications should not collect or use more data than what is required to provide their services or functions to the users. Moreover, this principle also requires that the applications should retain the users' data only for as long as it is needed to fulfill its intended purpose and delete or anonymize it afterwards. This principle is significant for mental health applications, as they deal with sensitive and personal information that can have significant implications for the users' well-being and privacy.
(5) **Quality and Integrity**: The principle of Quality and Integrity of data from FIPPs requires that the MHA that collect and process users' personal and health information (PII) should ensure its accuracy, relevance, and

completeness. This involves verifying, updating, correcting, and deleting the data as needed. This principle is crucial for ensuring fairness and respect for the users, as well as for providing effective and appropriate services or functions to them. It is particularly important for mental health applications, as they deal with sensitive and personal information that can impact the users' diagnosis, treatment, or well-being. Inaccurate, incomplete, or outdated data can lead to erroneous or harmful outcomes for the users, such as misdiagnosis, inappropriate treatment, or stigma. Therefore, ensuring the quality and integrity of the data is necessary for the MHA.

(6) **Individual Participation**: This principle requires that MHA obtain individual consent for the creation and processing of PII and PHI. This implies that individuals should be notified about the purposes and methods of data collection and use, and have the option to consent or deny the processing of their data. Furthermore, MHA should implement procedures for responding to and resolving individuals' privacy-related complaints and inquiries. Subsequently, individuals should have the right to contest or appeal any decisions or actions that impact their privacy rights. An appeals procedure ensure MHA respect the autonomy and preferences of their users and provide them with clear and transparent information and choices about their data practices.

(7) **Purpose Specification and Use Limitation**: MHA should provide notice of the specific purpose for which each PII is collected. This means that individuals should be aware of the reasons and objectives behind data collection and use. Moreover, MHA should only use, process, store, maintain, share, or disclose PII for a purpose that is explained in the privacy policy notice. This means that individuals should expect that their data will not be used for any other purposes than those stated in the notice, or for any purposes that are incompatible or inconsistent with them. In the context of mental health applications, it is essential to specify purpose for data collection and processing as it involved PII and PHI with significant implications for individuals' well-being.

(8) **Security**: The principle emphasizes the need for applications to implement safeguards to protect users' PII and PHI. This includes measures to prevent unauthorized access, modification, loss, disclosure, or exposure of information. The safeguards implemented should be appropriate and proportional to the level of harm that could be caused by incidents of breach or misuse. In case of privacy or data breach, organizations should have measures in place to assess the impact on individuals' privacy rights and apply adequate security controls. In the case of mental health applications, this principle is crucial since they deal with sensitive and personal data that can significantly affect users' well-being and dignity. Thus, it is vital for mental health applications to implement robust and reliable security mechanisms to safeguard user data.

(9) **Transparency**: This principle demands that MHA notify individuals of their data practices for PII and PHI. This covers the purposes and methods of data collection and use, the choices, and rights of individuals regarding their data, and the benefits and risks of data sharing with 3rd parties. The notice should also be accessible and understandable for individuals. This implies that organizations should disclose their data practices before or at the time of data collection and use. They should make the privacy policy notice readily available on the application download page, and the policy should be comprehensible without relying on technical jargon or legalese.

3 METHODOLOGY

This study utilized a sample of the top eight mental health smartphone applications on the Android platform to perform a privacy policy analysis. FIPPs served as the measuring scale to determine the degree to which these applications adhered to privacy-preserving principles.

Table 1. FIPPs analysis of Privacy Policies

Privacy Principles	*App 1*	*App 2*	*App 3*	*App 4*	*App 5*	*App 6*	*App 7*	*App8*
Access and Rectification	●	●	○	◑	○	●	●	○
Accountability	◑	○	○	○	○	◑	○	○
Authority	○	○	○	○	○	○	○	○
Minimization	○	○	○	○	○	○	○	●
Quality and Integrity	○	○	○	○	○	○	○	○
Individual Participation	◑	◑	◑	○	◑	●	◑	◑
Purpose Specification and Use Limitation	◑	○	◑	○	◑	◑	○	○
Security	◑	○	◑	○	●	◑	○	○
Transparency	○	○	○	○	○	●	◑	◑

Results from FIPPs analysis of Privacy Policies from selected Mental Health applications.
(LEGEND: ●= Followed, ◑= Partial, ○= Not followed)

3.1 Application Selection

The official application marketplace for Android is Google Playstore, which features various categories such as Health, Fitness, and Lifestyles, but does not offer a specific category for mental health applications. To identify mental health applications, search queries such as "mental health," "mental wellbeing," and "mental wellness" were utilized. The search was limited to English language applications and conducted with a US location setting. Based on ratings and the number of downloads, eight applications were selected from the search results, shown in Table 2.

3.2 Privacy Policy Assessment

We obtained the privacy policies of the selected mental health applications from their official pages on the Google Playstore. The availability of privacy policies on Google Playstore ensured easy accessibility to users. To assess the effectiveness of these policies in safeguarding user data, we employed the Fair Information Practice Principles (FIPPs) as a measure. The FIPPs principles were defined by the Federal Privacy Council (FPC) and the National Institute of Standards and Technology (NIST) which provide detailed guidance for managing privacy risk of user data [13, 23]. Additionally, we analyzed the privacy policies to determine their compliance with the (HIPAA), the and standard data regulation for covered health entities.

3.2.1 Policy Analysis. We employed a general inductive approach for qualitative analysis of the privacy policies of mental health smartphone applications [29]. Two researchers independently examined the policies and assessed them using FIPPs as a measuring scale. Following initial analysis, the researchers met and engaged in an iterative process to resolve any disagreements and ambiguities. Comment: a third independent researcher is conducting the analysis to confirm the result.

4 RESULTS

In the following sections, we will use share and describe our findings. Table 1 highlights the results from privacy policy analysis which are further described in detail below.

(1) **Right of Access and Rectification**: Our analysis revealed that only half of the applications respected these rights of the users. Among our selected mental health applications, three did not mention this right of access and

rectification at all in their privacy policies and one application allowed users to access their data but did not provide details on their right to amend any inaccurate or irrelevant data. The lack of right to amend also deprives users of the option to remove certain information that they are not comfortable in sharing with the application.

(2) **Accountability**: Our analysis of eight selected mental health applications revealed that only two of them partially addressed this principle in their policies, while the rest did not provide any information on their accountability mechanisms. Among the two applications that partially met this criterion, both specified the roles of their employees and third parties who deal with the users' personal and health information, but only one stated that they conduct audits and monitor their compliance with their privacy policy. None of the applications mentioned any training programs for their employee on how to manage sensitive PII and PHI information.

(3) **Authority**: Our analysis revealed that none of the eight selected mental health applications met this principle in their policies. No application specified who are the authorized individuals or entities that are responsible for accessing and managing the users' personal and health information. This creates ambiguity and uncertainty for the users about how their data is handled and by whom. It also raises questions about the accountability and transparency of the applications regarding their privacy practices.

(4) **Minimization**: Our analysis revealed that only one out of eight selected mental health applications adhered to this principle in their policies. The rest of the applications were found to be collecting device and social media identifiers of the users through various means, such as cookies, web beacons, or SDKs (Software Development Kits), and would even share this information with third parties (advertising and user analytics companies). Furthermore, some applications claimed to keep the users' data indefinitely or as long as it served their business purposes, instead of limiting the retention to only serve the users. These practices violate the principle of Minimization and expose the users' data to potential privacy breaches and harms.

(5) **Quality and Integrity**: Our analysis revealed that none of the eight selected mental health applications adhered to this principle in their policies. We observed that most of the applications did not make any efforts to keep the users' data accurate and relevant to ensure fairness, and a couple of applications claimed to do so but only for California residents in order to comply with the California Consumer Privacy Act (CCPA). Some applications even went as far as claiming that the responsibility of ensuring the relevance of the data collected (including device and social media identifiers) falls on the users and that the applications take no responsibility for it. These practices violate the principle of Quality and Integrity of data and expose the users' data to potential errors and discrimination.

(6) **Individual Participation**: Our analysis revealed that only one mental health application adhered to this principle fully. Among the other seven applications, six complied with this principle partially. Most of these six partial compliers had established procedures for addressing users' privacy queries and concerns, but they did not provide clear notice of user consent, or they limited the user consent to EU citizens in order to comply with the General Data Protection Regulation (GDPR). One application violated this principle completely. This suggests a disregard for users' choice, autonomy, and respect in the data practices of most mental health applications, posing threats to users' privacy rights and the security of their data.

(7) **Purpose Specification and Use Limitation**: Our analysis revealed that none of the selected eight mental health applications complied with this principle fully. Half of the applications followed this principle partially by providing a notice for the specific use of each PII and PHI they claimed to collect in the privacy policy, and the other half violated this principle completely. We found that the privacy policy failed to specify the use case of various collected PII and PHI, especially, not providing detail into how device and social media identifiers will be

used. Additionally, some applications did not provide details into the purpose for which PII and PHI were shared with third parties. This indicates a lack of transparency and accountability in the data practices of most mental health applications. It also poses threats to users' privacy rights and the security of their data.

(8) **Security**: Our analysis of privacy policies revealed that only one application adhered to this principle fully, while three applications complied with this principle partially. Four mental health applications violated this principle completely. Most of the violations did not describe how they handled sensitive PII and PHI in case of data and privacy breach. This further indicates a lack of security and accountability in the data practices of most mental health applications, putting users' privacy rights and the security at risk.

(9) **Transparency**: Our analysis showed that only one application adhered to this principle, one application complied with this principle partially, and five applications violated this principle completely. Our analysis revealed that most of the applications' privacy policies contained technical terminology and legalese that only domain experts could understand. Moreover, one application did not even provide their privacy policy on the Google Playstore and required manual search on their website, which further reduced accessibility. This indicates a lack of transparency and accountability in the data practices of most mental health applications. It also undermines users' trust and confidence in their data protection.

5 DISCUSSION

5.1 Lack of HIPAA Compliance

One of the criteria we used to evaluate the privacy policies of mental health applications was their compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a federal law that established national standards for protecting sensitive patient health information from unauthorized disclosure [11]. HIPAA applies to covered entities, such as health care providers, health plans, and health care clearinghouses, as well as their business associates, who use or disclose protected health information (PHI) in electronic form. PHI includes any information that relates to the past, present, or future mental or physical health or condition of an individual, or the provision or payment of health care to an individual [11].

Our analysis revealed that none of the applications in our sample claimed to comply with HIPAA. Some applications stated that they could work with users' insurance companies for medical assessments but did not provide any details on how they would ensure data security and privacy during the integration process. This raises concerns about the potential risks of data breaches, identity theft, or misuse of sensitive information for users who share their mental health data with these applications. It is important for mental health application to comply with HIPAA as it can increase users' trust and willingness to seek help, as well as protect their rights and autonomy [20].

5.2 Device and Social Media Data Collection

Our findings reveal a concerning situation in which mental health applications collect device and social media information of their users, without adequate privacy protections or transparency. This data, which may include sensitive information about users' moods, mental states, and biometric data, is vulnerable to privacy breaches and misuse when shared with third parties, such as advertisers or data brokers [17]. Such breaches could have serious consequences for users' mental health, well-being, and identity, as well as their trust and willingness to seek help [16].

5.3 Geographic Disparities in Privacy Rights

Our analysis revealed that some of the rights that FIPPs required, such as data minimization, purpose specification, and individual participation etc., were only guaranteed for EU citizens and California residents by the application privacy policies. This was mainly due to the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which incorporated FIPPs in their provisions [26]. This unequal treatment could result in other users being deprived of certain digital rights and being discriminated against based on their geographic location. In this context, a human might say that mental health application developers should apply FIPPs universally and consistently to all users, regardless of their legal jurisdiction, as a matter of ethical responsibility and best practice

6 LIMITATIONS

We designed this study as an exploratory study focusing on privacy policy to establish practical understanding of the application privacy principles in information technology. A detailed study with larger set of applications is needed to establish a more holistic picture of how the privacy policies perform in context of regulations and privacy principles. Additionally, we only focused on FIPPs as a measure of privacy, but for additional work, we plan to incorporate other more recent privacy frameworks such as CCPA, GDPR, and more recently newer privacy regulations by FTC in cyberspace [6]. The aim of this study was to explore privacy policy as a practical tool for communicating the application privacy principles in information technology. However, this study has some limitations that suggest directions for future research.

- First, we analyzed a small sample of applications, which may not be representative of the whole population of mental health applications. Therefore, a larger and more systematic study is needed to provide a more holistic picture of how privacy policies perform in relation to the existing regulations and privacy principles.
- Second, we used FIPPs as the main framework for evaluating the privacy policies, but we acknowledge that there are other more recent and relevant privacy frameworks that could be applied, such as CCPA, GDPR, and the newer privacy regulations by FTC in cyberspace [6].Thus, we plan to incorporate these frameworks into our analysis in our future work.
- Third, we relied on two reviewers to conduct the privacy analysis. In future, we aim to involve more reviewers and use inter-rater reliability measures to enhance the validity and reliability of our findings in the future extension of this work.

7 CONCLUSION

In conclusion, our study demonstrates that many of the popular and highly rated mental health applications (Table 2) have inadequate privacy policies that violate the FIPPs guidelines. They collect and use excessive and unnecessary data, jeopardize the integrity and security of users' sensitive PII and PHI, and fail to provide transparency and accountability mechanisms. These findings suggest a need for improved privacy design and regulation in the field of mental health applications. We aim to inform and inspire policy makers and mental health app developers to adopt more rigorous and user-centric privacy standards and practices. Policy makers can use our findings to address the gaps and challenges in the existing privacy regulations and frameworks, and to devise more effective and enforceable policies that safeguard the rights and interests of mental health app users. This can enhance the trust and confidence of their users, as well as their own reputation and social responsibility.

ACKNOWLEDGMENTS

To Robert, for the bagels and explaining CMYK and color spaces.

REFERENCES

[1] [n. d.]. COVID-19 pandemic triggers 25% increase in prevalence of anxiety and depression worldwide. https://www.who.int/news/item/02-03-2022-covid-19-pandemic-triggers-25-increase-in-prevalence-of-anxiety-and-depression-worldwide.
[2] 2022. HIPAA & Health Apps. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html.
[3] 2023. Mental Health Treatments. https://www.mhanational.org/mental-health-treatments.
[4] 2023. Mental Illness. https://www.nimh.nih.gov/health/statistics/mental-illness.
[5] American Psychological Association. 2021. Trends in mental health apps. https://www.apa.org/monitor/2021/01/trends-mental-health-apps
[6] A Boyd and Jessica L. Peel. 2022. Tech Transactions & Data Privacy 2022 Report: The FTC's Expanding Role in Cybersecurity and Data Privacy Enforcement in 2022 — natlawreview.com. https://www.natlawreview.com/article/tech-transactions-data-privacy-2022-report-ftc-s-expanding-role-cybersecurity-and.
[7] Pew Research Center. 2021. Mobile Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/mobile/
[8] CLOUDFLARE. 2023. What are the Fair Information Practice Principles (FIPPs)? https://www.cloudflare.com/en-gb/learning/privacy/what-are-fair-information-practices-fipps/.
[9] Tara Donker, Katherine Petrie, Judy Proudfoot, Janine Clarke, Mary-Rose Birch, and Helen Christensen. 2013. Smartphones for smarter delivery of mental health programs: a systematic review. *Journal of medical Internet research* 15, 11 (2013), e247.
[10] Office for Civil Rights (OCR). 2020. What is a covered entity's liability under the HIPAA Privacy Rule for sharing data inappropriately to or through a health information organization (HIO) or other electronic health information exchange network? | Guidance Portal. https://www.hhs.gov/guidance/document/faq-537-what-covered-entitys-liability-under-hipaa-privacy-rule-sharing-data.
[11] Office for Civil Rights (OCR). 2022. Summary of the HIPAA Privacy Rule. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
[12] Mozilla Foundation. 2022. Top mental health and prayer apps fail spectacularly at privacy & security. https://foundation.mozilla.org/en/blog/top-mental-health-and-prayer-apps-fail-spectacularly-at-privacy-security/
[13] The Federal Privacy Council (FPC). 2022. Fair Information Practice Principles (FIPPs) | FPC. https://www.fpc.gov/resources/fipps/.
[14] Panagiota Galetsi, Korina Katsaliaki, and Sameer Kumar. 2023. Exploring benefits and ethical challenges in the rise of mHealth (mobile healthcare) technology for the common good: An analysis of mobile applications for health specialists. *Technovation* 121 (2023), 102598.
[15] Thomas Germain. 2021. Mental Health Apps and User Privacy. https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/
[16] GoodTherapy. 2020. HIPAA for Mental Health Professionals: The Basics. https://www.goodtherapy.org/for-professionals/software-technology/hipaa-security/article/hipaa-for-mental-health-professionals-the-basics
[17] Tatum Hunter and Jeremy B. Merrill. 2022. Health apps share your concerns with advertisers. HIPAA can't stop it. https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/.
[18] Leonardo Horn Iwaya, M Ali Babar, Awais Rashid, and Chamila Wijayarathna. 2023. On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering* 28, 1 (2023), 2.
[19] Ellen E Lee, John Torous, Munmun De Choudhury, Colin A Depp, Sarah A Graham, Ho-Cheol Kim, Martin P Paulus, John H Krystal, and Dilip V Jeste. 2021. Artificial intelligence for mental health care: clinical applications, barriers, facilitators, and artificial wisdom. *Biological Psychiatry: Cognitive Neuroscience and Neuroimaging* 6, 9 (2021), 856–864.
[20] Samuel D Lustgarten, Yunkyoung L Garrison, Morgan T Sinnard, and Anthony WP Flynn. 2020. Digital privacy in mental healthcare: current issues and recommendations for technology use. *Current opinion in psychology* 36 (2020), 25–31.
[21] Melissa Madeson. 2021. Mobile Health Apps: Providing Better Care to Patients. https://positivepsychology.com/mobile-health-apps/.
[22] Wallace Mandell. 1995. Origins of Mental Health, The Realization of an Idea. *Johns Hopkins Bloomberg School of Public Health. Baltimore, MD: Johns Hopkins University* (1995).
[23] NIST. 2022. Privacy Framework — nist.gov. https://www.nist.gov/privacy-framework/privacy-framework.
[24] Cláudia Ortet and Liliana Vale Costa. 2022. "Listen to Your Immune System When It's Calling for You": Monitoring Autoimmune Diseases Using the iShU App. *Sensors* 22, 10 (2022), 3834.
[25] Andrea Rice. 2022. Can Mobile Phone Apps Improve Your Mental Health? https://psychcentral.com/news/mobile-phone-based-interventions-in-mental-health.
[26] Cheryl Saniuk-Heinig. 2021. 50 years and still kicking: An examination of FIPPs in modern regulation. https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/
[27] Statista. 2021. Number of free and paid mobile app store downloads worldwide from 2016 to 2020. https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/

[28] Mohammad Tahaei, Julia Bernd, and Awais Rashid. 2022. Privacy, permissions, and the health app ecosystem: A stack overflow exploration. In *Proceedings of the 2022 European Symposium on Usable Security*. 117–130.

[29] David R Thomas. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* 27, 2 (2006), 237–246.

[30] Tian Wang, Lin Guo, and Masooda Bashir. 2021. COVID-19 Apps and Privacy Protections from Users' Perspective. *Proceedings of the Association for Information Science and Technology* 58, 1 (2021), 357–365.

A APPLICATION SELECTION

Table 2. Selected Application Details

Application Name	***Number of Installs***	***Rating***	***Genre***
MindDoc: Your Companion	1,000,000+	4.2	Medical
Sanvello: Anxiety Depression	1,000,000+	4.6	Medical
Mental Health Tests	500,000+	4.3	Medical
Calm - Sleep, Meditate, Relax	50,000,000+	4.4	Health Fitness
Headspace: Mindful Meditation	10,000,000+	4.5	Health Fitness
Finch: Self Care Pet	1,000,000+	4.9	Health Fitness
Balance: Meditation Sleep	1,000,000+	4.8	Health Fitness
Daylio Journal - Mood Tracker	10,000,000+	4.7	Lifestyle