Privacy Policy Framework for Indian Mental Health Apps

January 9, 2025

By Chakshu Sang and Shweta Mohandas

Reviewed by Pallavi Bedi and Isha Suri
Copy Editing - The Clean Copy

The Centre for Internet and Society, India

https://cis-india.org

Chapter 1: Introduction

Technology development has made services and solutions available to people at their fingertips, including the ability to purchase goods and services for one's physical and mental well-being. Over the last decade, the number of mental health apps available globally has increased exponentially. A study conducted in 2012, revealed that just 6% of 9,000 (540) health-related apps targeted mental health concerns. By 2020, a similar study reported that number to have increased to 10,000 apps with an increased focus on symptom tracking, habit formation, and other areas. The number of apps available and their uptake have increased, especially since the COVID-19 pandemic.[1] These apps provide a range of services such as one-to-one counselling with a professional, digital version of mental health exercises, and chatbot-based mental health support to name a few, to improve the well-being of their users at the touch of a few buttons.

An essential part of any app is its privacy policy, which informs users of how it collects and uses their data. An international study on users' awareness of privacy concerns indicates that they are not always aware of the rights they are giving up while consenting to a privacy policy or the purpose of such policies.[2] Understanding the terms of a privacy policy is important, especially for mental health apps, which deal with sensitive personal information.

This report analyses the privacy policies of mental health apps in India and provides recommendations for making the policies not only legally compliant but also user-centric. The report's findings indicate a significant gap in the structure and content of privacy policies in Indian mental health apps. This highlights the need to develop a framework that can guide organisations in developing their privacy policies. Therefore, this report proposes a holistic framework to guide the development of privacy policies for mental health apps in India. It focuses on three key segments that are an essential part of the privacy policy of any mental

[1] Rebecca A. Clay, "Mental Health Apps Are Gaining Traction", *Monitor on Psychology* 52, no. 1 (2021): 55, https://www.apa.org/monitor/2021/01/trends-mental-health-apps.
[2] Tommy Nguyen, Garnet Yeates, Tony Ly, and Umar Albalawi, "A Study on Exploring the Level of Awareness of Privacy Concerns and Risks", *Applied Sciences* 13, no. 24 (2023): 13237, https://doi.org/10.3390/app132413237.

health app. First, it must include factors considered essential by the Digital Personal Data Protection Act 2023 (DPDPA) such as consent mechanisms, rights of the data principal, provision to withdraw consent etc. Second, the privacy policy must state how the data provided by them to these apps will be used. Finally, developers must include key elements, such as provisions for third-party integrations and data retention policies.

1.1 Definition of mental health

According to the World Health Organization (WHO), mental health is a state of mind that allows individuals to cope with stressors, understand their strengths and skills, and contribute to the community.[3] According to the Indian Mental Healthcare Act 2017 (MHA), mental healthcare involves analysing an individual's mental status and providing adequate treatment and rehabilitation for their symptoms and condition.[4] It does not distinguish between in-person and digital healthcare initiatives. Few other definitions related to mental health speak about " well-being" and describe it as how an individual perceives oneself, deals with adversities, and engages with opportunities in various dimensions of life, such as the workplace, community, or family.[5] Therefore, understanding mental health apps requires a clear grasp of the concept of digital mental health and the broader global context in which these apps operate.

According to the American Psychiatric Association, digital mental health involves the use of digital techniques for the management of mental health concerns, provision of interventions between sessions, promotion of mental well-being, and treatment of mental health concerns through digital and online mechanisms.[6] Mental health apps provide a range of digital mental health interventions in one place, such as digital journaling and diaries, peer support communities, therapeutic interventions, mood tracking, psychoeducational resources, and more.[7] These digital mental health interventions provide anonymity to users as the apps allow individuals to customise their names. They also provide access to mobile-based online

---

[3] "Mental Health," *World Health Organization*, accessed 29 December 2024, https://www.who.int/health-topics/mental-health#tab=tab_1.
[4] The Mental Healthcare Act, 2017.
[5] Dinesh Bhugra, Alex Till, and Norman Sartorius, "What Is Mental Health?" *International Journal of Social Psychiatry* 59, no. 1 (2013): 3–4, https://doi.org/10.1177/0020764012463315.
[6] "Digital Mental Health", *American Psychiatric Association*, accessed 29 December 2024, https://www.psychiatry.org/psychiatrists/practice/digital-mental-health.
[7] Raymond R. Bond, Maurice D. Mulvenna, Courtney Potts, Siobhan O'Neill, Edel Ennis, and John Torous, "Digital Transformation of Mental Health Services", *npj Mental Health Research* 2, no. 1 (2023), https://doi.org/10.1038/s44184-023-00033-y.

sessions and allow users to tailor the app according to their requirements as a first step towards taking charge of their mental health.

1.2 Background

The National Institute of Mental Health (NIMH), a globally recognised institution focused on mental health situated in the US, classifies mental health apps can be classified into the following six categories based on their functionality:[8] These groups include:

1. Self-management, where an individual manages their symptoms and well-being with the help of feedback from the app
2. Cognitive improvement, where an individual improves their thinking skills and works on severe mental health conditions
3. Skills training, where an individual engages with techniques using the app to work on their mental health – for example, by learning about coping mechanisms or addressing negative thinking
4. Supported care, where an individual interacts with mental health professionals and other members of their peer community through the app
5. Symptom tracking, where an individual tracks their conditions and symptoms
6. Passive data collection, where symptoms of the individuals are tracked through in-built mechanisms in the phone or the app thus acquiring large amounts of data from the users without their active inputs

Mental health apps are popular for many reasons: ease of access, portability of mental health support, the reduced effort required to care for one's well-being, and more.[9] Studies indicate that such apps might enhance self-awareness, increase autonomy,[10] and support the destigmatisation of mental health.[11]

---

[8] "Technology and the Future of Mental Health Treatment", *National Institute of Mental Health*, accessed 29 December 2024, https://www.nimh.nih.gov/health/topics/technology-and-the-future-of-mental-health-treatment.
[9] Pooja Chandrashekar, "Do Mental Health Mobile Apps Work: Evidence and Recommendations for Designing High-Efficacy Mental Health Mobile Apps", *mHealth* 4 (2018): 6, https://doi.org/10.21037/mhealth.2018.03.02.
[10] Jennifer L Prentice and Keith S. Dobson, "A Review of the Risks and Benefits Associated with Mobile Phone Applications for Psychological Interventions", *Canadian Psychology/Psychologie Canadienne* 55, no. 4 (2014): 282–90, https://doi.org/10.1037/a0038113.
[11] David Bakker, Nikolaos Kazantzis, Debra Rickwood, and Nikki Rickard, "Mental Health Smartphone Apps: Review and Evidence-Based Recommendations for Future Developments", *JMIR Mental Health* 3, no. 1 (2016): e7, https://doi.org/10.2196/mental.4984.

While these apps have multiple benefits, they also have certain shortcomings – for instance, some apps may be less secure in terms of protecting users' data.[12] These apps may also be created by developers who are unaware of data security concerns. Furthermore, developers might not have the time to build adequate protection against data leaks when required to develop apps within quick turnaround times.[13] Relying on advertising and analytical third parties can also contribute to data leaks and the re-identification of personal data.[14]

[12] Leonardo Horn Iwaya, M. Ali Babar, Awais Rashid, and Chamila Wijayarathna, "On the Privacy of Mental Health Apps", *Empirical Software Engineering* 28, no. 1 (2022), https://doi.org/10.1007/s10664-022-10236-0.
[13] Bakheet Aljedaani and M Ali Babar, "Challenges with Developing Secure Mobile Health Applications: Systematic Review", *JMIR mHealth and uHealth* 9, no. 6 (2021): e15654. https://doi.org/10.2196/15654.
[14] Iwaya et al., "On the Privacy of Mental Health Apps".

Chapter 2: Methodology

For this study, we conducted desk research on the publicly available privacy policies of mental health apps available in India. We adopted the definition of mental health apps provided by the US National Institute for Mental Health (NIMH) for the current study.

We identified an initial pool of 737 mental health apps on the Apple App Store and Google Play Store. Keywords such as 'mental health', 'anxiety apps', and 'depression apps' were used to identify the sample apps. We removed duplicates and arrived at a list of 185 apps. These apps provide all forms of mental health services, including evidence-based therapeutic techniques (e.g., Cognitive Behaviour Therapy [CBT], Rational Emotive Behaviour Therapy [REBT], Acceptance and Commitment Therapy [ACT]), one-on-one online sessions via chat or calls, artificial intelligence (AI) chatbot-guided exercises, and community support for peer interaction and guidance. Some also offer other wellness and relaxation-based techniques, such as mindfulness and meditation. Based on the services provided, we formulated inclusion and exclusion criteria for the study and categorised the apps.[15]

2.1 Inclusion criteria

We included apps created both in India and other countries, which provide services in India. We only included apps that support mental health through established mental health exercises or sessions with a mental health professional. To be included, the app or mental health service had to be well established through high ratings and reviews such as acquiring a 4+ star rating in the app stores or recognition in the public domain (articles in journals or accolades).

2.2 Exclusion criteria

Other apps were excluded based on the exclusion criteria detailed below. Firstly, we excluded apps providing services such as mindfulness, meditation, journaling, and mood tracking as the sole feature. We did this to narrow the focus of the study from well-being-related techniques to psychotherapy approaches. Secondly, mental health games provide therapeutic interventions through different delivery formats than other apps. Hence, we excluded them.

---

[15] Kit Huckvale, Jennifer Nicholas, John Torous, and Mark E Larsen, "Smartphone Apps for the Treatment of Mental Health Conditions: Status and Considerations", *Current Opinion in Psychology* 36 (2020): 65–70, https://doi.org/10.1016/j.copsyc.2020.04.008.

Thirdly, we excluded apps that did not use established mental health techniques. Finally, we also excluded apps that did not have at least 100 reviews or were not available for download – this suggested a small user base and or the app might be unreliable or irrelevant to users.

Based on the inclusion and exclusion criteria, we included 52 apps for review – 34 Indian and 18 international. When we reviewed the privacy policies of the 52 apps, we further excluded 7 apps from the analysis for several reasons. One app had discontinued its services, and the organisation was no longer functional. Six other apps had not published a privacy policy on their app page or website.

Therefore, the final list of apps analysed included 45 apps: 28 from India and 17 others from abroad. Of the international apps, 11 were from the US, 1 from Canada, 2 from the United Kingdom, 2 from the European Union, and 1 from Singapore. Please see the Annexure for the final list of apps.

2.3 Data extraction and analysis

We created an app evaluation form for data extraction and analysis. The form captured general information about the app and details about its privacy policy – such as the data collection methods used, data usage, data security measures, and the presence of third-party sharing. By doing so, we aimed to capture commonalities in the privacy policies of Indian and international apps and collate unique policy inputs, such as best practices, to formulate a framework for developing privacy policies for mental health apps in India.

We undertook descriptive and quantitative content analyses of the data. This process helped us identify privacy policy trends, patterns, and themes, including data collection, security measures, and data sharing. We also noted the specific methods and similar approaches used for the aforementioned aspects of the app. We assessed the privacy policies and extracted the data between the end of May 2024 and mid-August 2024. After that, we undertook the analysis between August and September 2024.

2.4 Study limitations

We understand that there may be other mental health apps that might be available in India that the study has not covered. Further, we only studied the publicly available privacy

policies of these apps and did not examine the actual implementation of the policy. We also acknowledge that this report is being drafted and published at a time when the DPDPA has been passed, but it has not yet been implemented, and the rules have not yet been published. We have tried to assess the apps using the parameters mentioned in the DPDPA, in addition to further sector-specific guidelines. While several helplines provide mental health support, we did not include them in this study due to their complexity and opaqueness of processes. We limited our analysis to digital mental health interventions through mental health apps.

Chapter 3: Findings

For this report, 45 apps qualified for a detailed review of their privacy policies; of these, 28 were Indian apps, and 17 were international apps. Our analysis revealed significant insights into their data collection, data sharing, security mechanisms, and areas of compliance with laws, seeking user consent, and users' rights.

3.1 Data collection

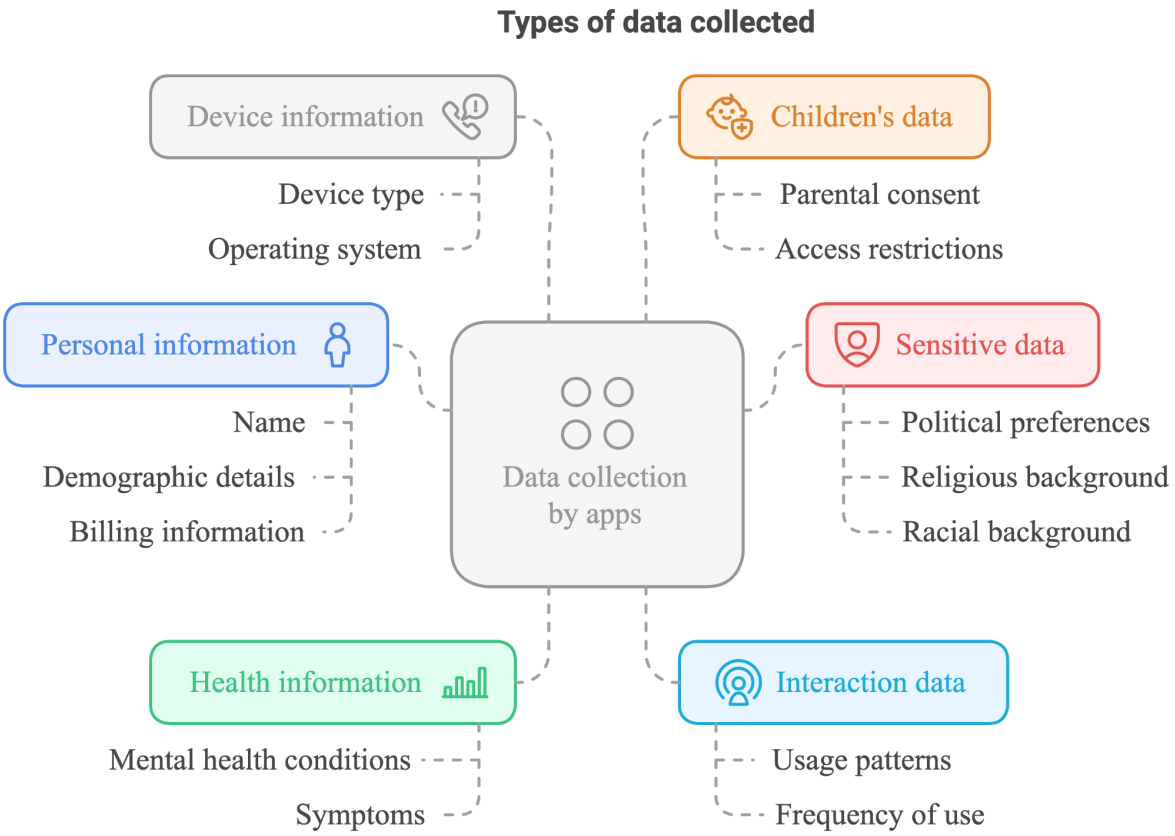
Mental health apps collect user information across various categories, including demographic details, health information, interaction patterns, device information, and sensitive personal data. Our findings indicate that all apps acknowledge collecting basic personal information ranging from name and demographic details to the necessary billing information (in the case of paid apps). While all international apps also collect interaction data, such as usage patterns, frequency, and device information, only 86% of Indian apps collected similar data.

Mental health apps collect data such as users' signs and symptoms, daily app interaction information, moods, mental health assessments, and responses to questionnaires and surveys to support self-monitoring and management features. We found that 80% of the reviewed apps gathered users' health information, such as mental health conditions and symptoms.

A few apps permit their use by children between 13 and 18 years of age with parental consent and supervision. In our analysis, about 18% of international apps and 14% of Indian apps permit the collection of children's data.

Figure 1 presents an overview of the data collected by mental health apps and the specific types of data they collect under each category.

Figure 1: Types of data collected by mental health apps



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

3.2 Use of data

All the apps we analysed stated that they process user data to provide services. In their privacy policies, 71% of Indian apps stated that they used the data to research the app's features, such as its efficacy, compared to 53% of international apps.

Advertising and marketing are other primary uses of data in apps, with 60% admitting that they used the data for advertising. Other uses of data include clinical oversight, creating follow-ups, and monitoring usage trends.

The results also indicate that 80% of the reviewed apps use data to provide a customised user experience. To facilitate a customised experience, 68% of Indian and 88% of international apps acknowledge observing the behavioural trends of users.

3.3 Use of data during emergencies

Our study found that 62% of all the apps highlight that they would use the individual's data during emergencies, including the safety of the user or others, a threat to their property, risk of harm, or suspected cases of abuse or neglect. However, we noted that 51% of the apps did not have specific protocols for sharing information during emergencies. The remaining apps indicated following protocols based on legal compliances and sharing the information with relevant official authorities.

3.4 Sharing of data

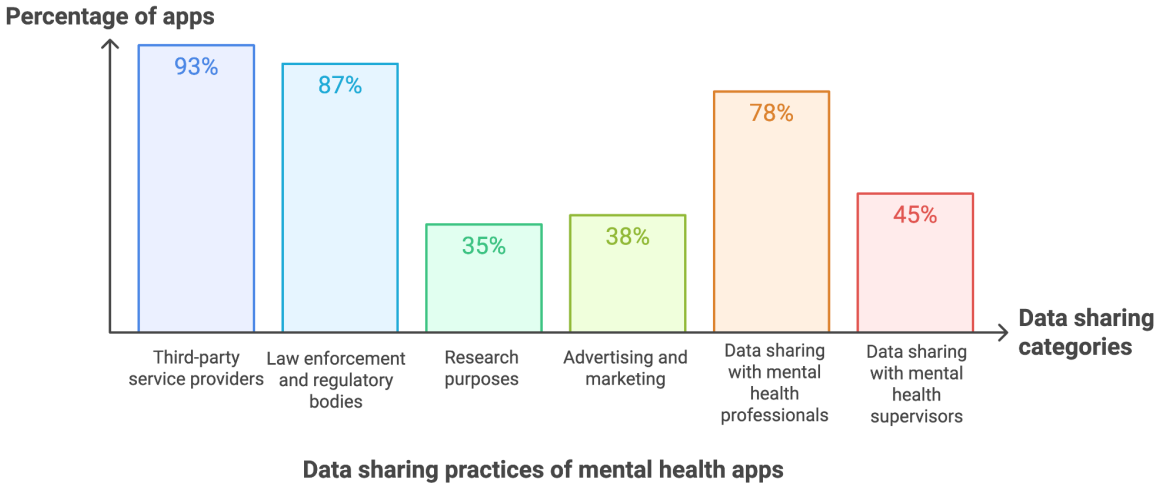
The results indicate that 93% of all the apps mention sharing users' data with third-party service providers; 87% mention sharing data with law enforcement and regulatory bodies. Additionally, apps also share data with third parties for research (35%) and advertising and marketing purposes (38%).

We observed that 35% of the international apps specified in their policies that they would share the data in the event of a sale or merger of the company; only 14% of the Indian apps specified this.

Mental health apps also allow interactions with professionals – about 75% of Indian apps and 18% of international apps include consultations with mental health professionals. Of the apps offering professional consultation services, 78% state in their privacy policies that they share the users' data with mental health professionals (MHPs) and 45% with mental health supervisors (See Figure 2).[16]

Figure 2: Who has access to data from mental health apps

[16] Supervisors are mental health professionals with greater levels of experience who have been practising in the field for years.



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

3.5 Security mechanisms

In 52% of the apps we studied, their privacy policy mentioned using encryption to keep an individual's data secure; 39% mentioned using anonymisation techniques. While sharing the individual's personal information with mental health professionals, some apps specify using secure socket layer (SSL) encryptions or other industry-standard security mechanisms. Of the apps that interact with professionals, only 24% of the Indian apps defined additional security measures implemented to secure the data collected and stored through such features. Furthermore, just 7% of the Indian apps acknowledged that they would inform their users in the event of a data breach or observation of suspicious activity in their accounts.

Our findings reveal that just 18% of international apps and 14% of Indian apps mention the provision of retaining user's data in the event of termination or discontinuation of the app and its services. While the number of apps making such data retention provisions is at par for Indian and international apps, the process of irreversible anonymisation while retaining such information differs. For instance, 18% of international apps specify adopting irreversible anonymisation when retaining data following the termination of the account or the app, while only one Indian app mentions implementing such a measure.

3.6 Rights of the users

a. *Right to access data*

All international apps mention allowing users to access their data, compared to 64% of Indian apps. Similarly, all international apps allow users to delete their data, compared to

82% of Indian apps. Only 18% of Indian apps allow data portability, compared to 94% of international apps.

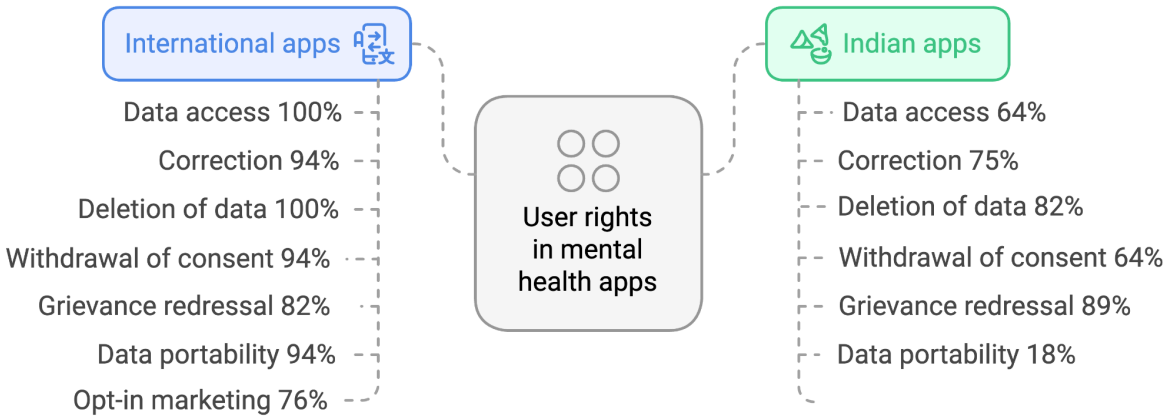
b. Right to correction and withdrawal of consent

About 94% of international apps state that users can correct inaccuracies in the information collected, compared to 75% of Indian apps. Likewise, 94% of international apps also allow users to withdraw consent, compared to 64% of Indian apps. We found that only 6% of international apps stated that users could opt-in for marketing material, compared to 21% of Indian apps.

c. Right to grievance redressal

We observed that 89% of Indian apps provide users access to grievance redressal support, compared to 82% of international apps.

Figure 3: Comparison between Indian and international mental health apps providing specific rights to users



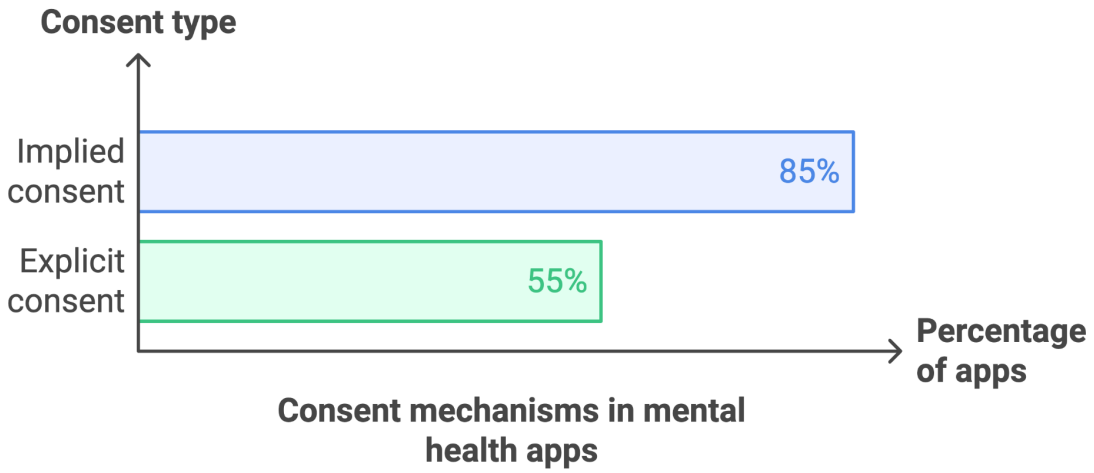
Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

3.7 Consent mechanisms

The results indicate that about 85% of the reviewed apps follow implied consent mechanisms (for instance, a consent option in the form of a pop-up box instead of a detailed list for the user to check and select). We also found that just 55% of the apps employ explicit consent techniques for users to agree to the privacy policy terms (for instance, a one-time or repeated

consent is obtained from the user when checking a pop-up box.) In explicit consent, an explicit agreement is sought regarding the app's policies and every update and change it makes. However, in the event of compliance with specific legal requirements, over 87% of all apps suggest processing the user's data without explicit consent. Hence, our results reveal that apps seem to use a combination of implied and explicit consent mechanisms.

Figure 4: Consent mechanisms in mental health apps



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

3.8 Language provisions

We found that 95% of the apps do not provide users with a privacy policy in a language other than English. Only one app specifies the alternate languages in which it offers services: Spanish and Hindi.

3.9 Transfer of data

Our analysis found that 61% of Indian apps do not mention whether they will transfer data outside India. The remaining 39% of Indian apps did not elaborate on the reasons for transferring data outside India. All the international apps mention the transfer of data. Organisations that transfer data outside India suggest adopting adequate safeguards such as standard contractual clauses (SCCs), data processing agreements (DPAs), encryption, and other industry-standard security measures during data transfer. They typically mention the US and the UK as the general locations for data transfer.

3.10 Changes to privacy policy

We found that 84% of all apps have provisions for informing users about changes in their privacy policies. Of these, 60% specify that they will provide some form of notice to users in the app or website and 22% state that they would also notify the user via email.

3.11 Data protection impact assessment (DPIAs) and data protection officer (DPO)

Comparatively, more international apps (29%) provide for the presence of a data protection officer than Indian apps (4%). Only one app, which has its origins and services in India and the UK, mentions that it conducts DPIAs.

3.12 Third-party integrations

We found that 39% of the Indian apps do not specify the type of third-party vendors used to provide their services. Some of the types of data they share with these third-party entities include personal data such as demographic information, payment and billing information, app usage, and device information. Only 12% of apps disclose the security protocols they implement while sharing such data with third-party entities. These protocols include confidentiality agreements based on data protection laws, but other security measures are vague and lack elaboration, implying only general privacy guidelines protocols.

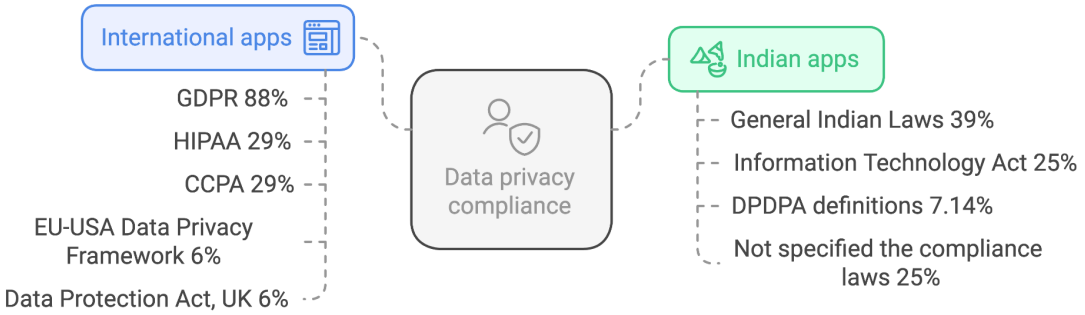
3.13 Compliance with the law

A few of the privacy policies of the Indian mental health apps disclose that they comply with various data protection laws such as the Indian Information Technology Act of 2000, Indian Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, and the EU's General Data Protection Regulation (GDPR) 2016. About 39% of Indian apps mention complying with "general Indian laws" without specifying the specific law. Interestingly, two Indian apps (7.14%) mention that they comply with some of the definitions specified in the DPDPA. While 25% of Indian apps adhere to the Information Technology Act, 25% failed to specify compliance with any data protection laws.

Most international apps indicate compliance with multiple global data protection laws; each app complied with at least one law. About 86% of international apps disclosed compliance with GDPR; 29% also said that they comply with the US Health Insurance Portability and Accountability Act (HIPAA) and California Consumer Privacy Act (CCPA); 6% mentioned

compliance with other laws such as the EU-US Data Privacy Framework and UK Data Protection Act.

Figure 5: Compliance of mental health apps with various data protection laws



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

These findings provide key insights into understanding the provisions of the privacy policies of the mental health apps available in India. From this data, certain gaps and areas of improvement emerge that can be further worked upon as well as researched.

Chapter 4: Discussion

Our review of mental health apps' privacy policies revealed an overall commitment to ensuring the privacy of people who access their services. However, our findings also suggest that not all apps are transparent about how they process and share data. Given the sensitive nature of the issue and the information they collect, a higher threshold for data protection and privacy is imperative. This section discusses how privacy policies could be more transparent and help people make informed choices.

4.1 Data collection

The apps gather users' personal and interaction data, including demographic details, symptoms and intensity, and mental health concerns. They must clarify this in their privacy policies. Individuals signing up for these apps should be aware of the data they collect, as this could also result in incorrect diagnoses, harming them further.

With online apps, it is also challenging to verify if the user is an adult and, thereby, have instances where minors use the app. Questions also arise regarding the extent of data collection for minors and the need for parental consent and supervision as a mandatory requirement before accessing the app's services. While some apps also cater to teenagers, there is a need to include provisions to ensure that minors' data are not shared or processed beyond what the app requires.

Additionally, apps must explore options for data minimisation and purpose limitation, which the DPDPA covers. This is particularly crucial when applications gather information, such as previous mental health diagnoses, from users during the onboarding stage.

4.2 Use of data for general use and emergencies

Mental health apps use data for various purposes, including providing and developing services, conducting research, advertising, and addressing emergencies. Therefore, their privacy policies must identify and specify the type of information used during such scenarios. For example, when it comes to demographic data, app interactions, or behavioural trends, it is essential for the app to specify the precise data that the organisation utilises and shares for its services. This ensures that users are informed about what data will be shared upon joining.

Organisations should also elaborate on how they use conversations internally to improve their systems, such as enhancing the effectiveness of AI chatbots or providing more tailored user services.

Many privacy policies mention utilising user data during emergencies. However, what constitutes an emergency is left vague. An emergency may arise from a political situation, worsening mental health, or a user's mental health crisis. In such situations, there can be a risk to their health and well-being along with that of others. In the case of self-injury, an escalation protocol must be established regarding the user's data. Furthermore, though the privacy policies state that the apps might share data with law enforcement agencies, it is unclear if they would share it at the agency's request or automatically during an emergency. Therefore, apps must clarify what constitutes an emergency and the actions they will take in such situations.

4.3 Data security

The apps claim to have several different security measures in place; however, our analysis reveals that these are described in vague terms. For instance, apps use terms such as 'general standard mechanisms' without providing any details.

The privacy policies of international apps are comparatively more detailed on security measures and appear more robust than those of their Indian counterparts. We found that Indian apps have vague security protocols that mention more standard practices. Given that international apps must adhere to global regulations such as GDPR and hence have stringent security measures, Indian apps should still ensure that adequate security measures are implemented.

4.4 Rights of the users

Our analysis revealed that Indian and international apps equally provide sufficient details about specific rights to their users, such as correcting inaccuracies in data, deleting data, and grievance redressal. Regardless, there is a moderate difference between them in the case of rights, such as user access to their data and withdrawal of consent, where the international apps perform better than the Indian apps. Many international apps offer users the right to opt in for marketing and data portability at a much higher rate than Indian apps. While Indian

apps flag a few essential rights, there is scope for improvement. While notices such as privacy policies are often seen as a way to opt into certain services, it should also include provisions to withdraw or opt out of the services. Given the sensitivities surrounding mental health data, apps should be transparent about using automated means for data processing or provide the option to opt out of such processing.

4.5 Consent mechanisms and language provisions

As we noted in the findings, most apps accepted implied consent as a form of consent mechanism requiring no feedback from the individual to record consent; often, these are in the form of privacy policies on the website or the app. Furthermore, using legal jargon and technical terms and having them only in one language (English) brings into question the level of understanding behind the consent provided by the user.

To ensure informed consent, apps must design and draft privacy policies that allow individuals to make an informed choice about whether to sign up for the app's services. These policies could be in multiple languages and simplified to understand and follow. Privacy policies must also be accessible to people with various accessibility needs.

4.6 Data protection impact assessments (DPIAs) and Data Protection Officer (DPO)

A data protection impact assessment identifies risks and ensures that apps securely handle user data. A data protection officer monitors and supports the organisation through compliance requirements and handles users' concerns and complaints regarding their data. According to international laws such as the GDPR, organisations must have a DPO, especially where individuals are monitored regularly or are part of a large public body. According to the DPDP Act, only significant data fiduciaries in India are required to conduct DPIAs and have a DPO.

Given the sensitive nature of health data and, more importantly, mental health data, mental health apps should be regulated as significant data fiduciaries. The data they collect and process should be subject to more stringent compliance requirements, including the need for a DPO.

Chapter 5: Framework for privacy policies

Based on our findings and discussions, we propose a framework to guide the drafting of privacy policies for mental health apps. Current legislation in India and globally centres on data collection and the overall protection of health-related information. However, due to the sensitive nature of mental health data, it requires particular focus. In India, the exclusion of sensitive personal data from the scope of DPDPA, which earlier provided increased responsibility for data fiduciaries, is a cause for concern. While we await the implementation of the DPDPA and the Rules, we propose a framework for privacy policies of mental health apps based on the provisions of the DPDPA, the components unique to mental health apps, and international best practices in mental health apps.

The recommended framework for mental health apps has three main segments. First, policy drafters must make special provisions for components and features unique to mental health apps. Second, the DPDPA's existing legal requirements necessitate the inclusion of specific components in privacy policies such as the provisions for withdrawal of consent, the need for privacy policies to be in Indian languages etc. that the policy drafters must incorporate. Third, developers of India's mental health app should reference the best practices found in the privacy policies of international apps that comply with regulations beyond the DPDPA when drafting their privacy policy.

5.1 Segment 1: Guidelines under different data protection laws

5.1.1 Clear visibility of the privacy policy

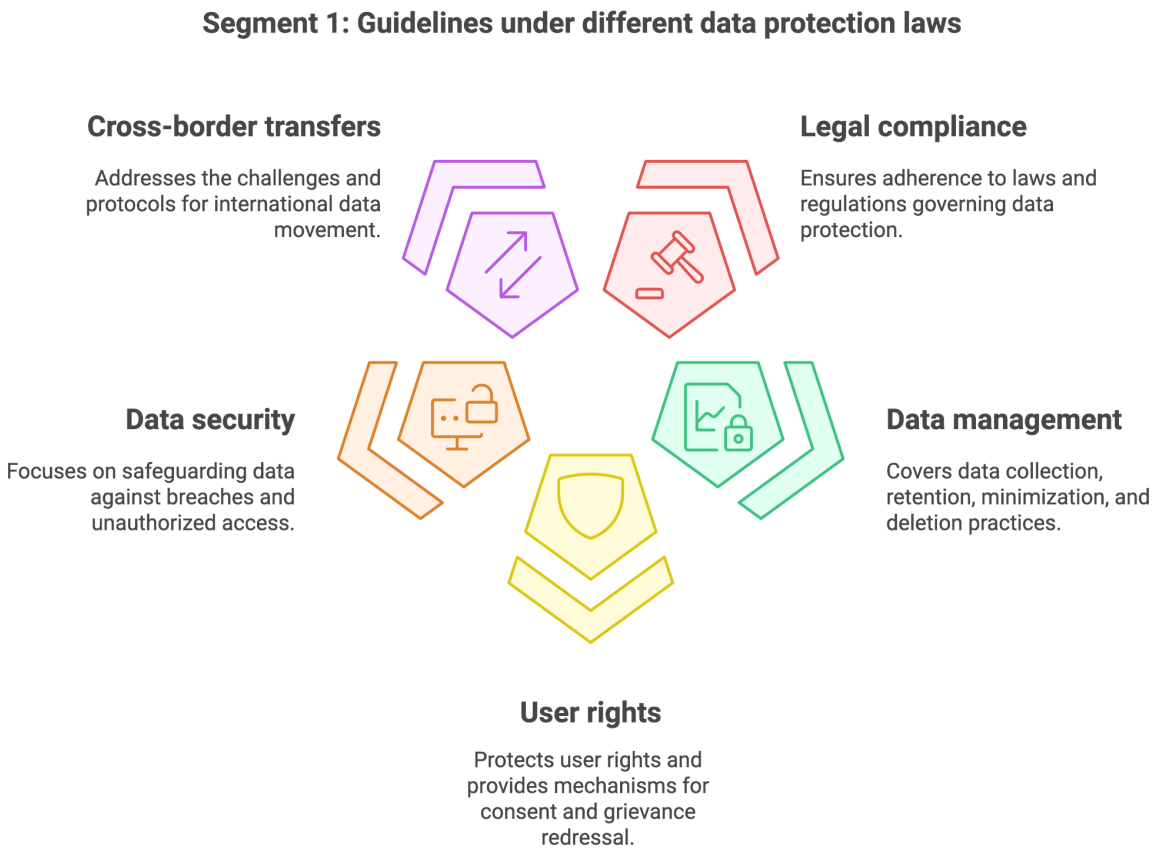
The privacy policy should be clearly visible and easily identifiable on the app and website. The platform should display this information in bold format with a visible font size and colour, accompanied by a hyperlink to the detailed document. Even if the link to the policy remains in the footer, it should be most 'obviously' visible to allow the user to access the document easily.

5.1.2 Clarity on terminology

The privacy policy must define any terminology or jargon used and specify the scope of those terms at the beginning of the document. For example, organisations should clearly define the

role and scope of a supervisor of the mental health professional employed/providing their services to the app in addition to explaining key terms in the document such as online chat, peer support community, and emergency. For example, rather than merely assuring compliance with general laws or implementing ‘standard’ security measures, the policy must specify the exact laws it adheres to and the precise mechanisms it employs, avoiding vague descriptions.

Figure 6: Guidelines under different data protection laws constitute the key components of Segment 1.



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

5.1.3 Grouping of information

App developers must categorise all information in the privacy policy into sections. This will allow for easy understanding, quick analysis, and navigation. Although the DPDPA is yet to be implemented, developers should still adhere to its provisions while waiting for the Rules.

For instance, according to the DPDPA, the following components need to be incorporated in privacy policies:

a. *Compliance to laws*

   The DPDPA requires the privacy policy to specify the data protection laws it complies with. It must specify all the relevant laws if it complies with multiple laws specific to different countries where it provides its services.

b. *Types of data collected*

   The privacy policy must specify the details of all the data collected by the mental health app, including personal information, data on mental health conditions, devices, and sensitive information. This information should be comprehensively categorised rather than mentioned randomly without any order.

c. *Purpose of data collection*

   Under this section, apps must highlight the purpose for which the data will be used. For instance, if the app plans to use the data for research, service development, or advertising, it must inform the users beforehand through the policy.

d. *Consent mechanisms*

   The privacy policy must clearly disclose the app's consent mechanism, particularly if the mechanisms differ for different purposes. For example, the details must be mentioned if consent for research is more explicit than for using services, which might be more implicit.

e. *Children's data*

   Any mental health app collecting children's data must detail the protocols followed in such scenarios. The app must specify the age group from which data is collected, the security protocols followed to safeguard the collection and storage of data, and the specific consent mechanism used to acquire such data. If an app does not collect children's data and ends up collecting it inadvertently, the policy must include adequate processes to delete it, including the timeframe for action, security protocols, and access restrictions.

f. Data minimisation

The policy must define minimisation and highlight data minimisation practices, including the mechanisms the app uses to prevent unnecessary data collection.

g. Data retention and data deletion

The app should clearly define its practices for securely storing and deleting data from its servers. It must provide the rationale for storing the data and detail the process and timeframe for data retention and deletion.

h. User rights

The policy must list and explain the users' rights, such as their right to access their data, request corrections and erasure, and provide details about data processing.

i. Data security

- The policy must specify the security measures implemented in the app, including details of the measures used, such as the ISO standards. If the app uses different mechanisms for various services, it must provide detailed information on all the procedures rather than generalised statements.
- The policy should also share how it will protect the user's shared data and the mechanisms it involves.

j. Data breach

This section of the policy must detail the actions the app takes during a data breach. It must specify the timeframe for action, the process followed, the officials involved in such an incident, and the mechanism for informing the users and officials about a data breach.

k. *Cross-border data transfers*

The policy must highlight the process of transferring data outside of India, including specifications of the countries where the data is transferred and the transfer mechanisms. It must also communicate to users the adoption of specific standards, such as Standard Contractual Clauses. The policy must also specify the data security processes during such transfers.

l. *Grievance redressal*

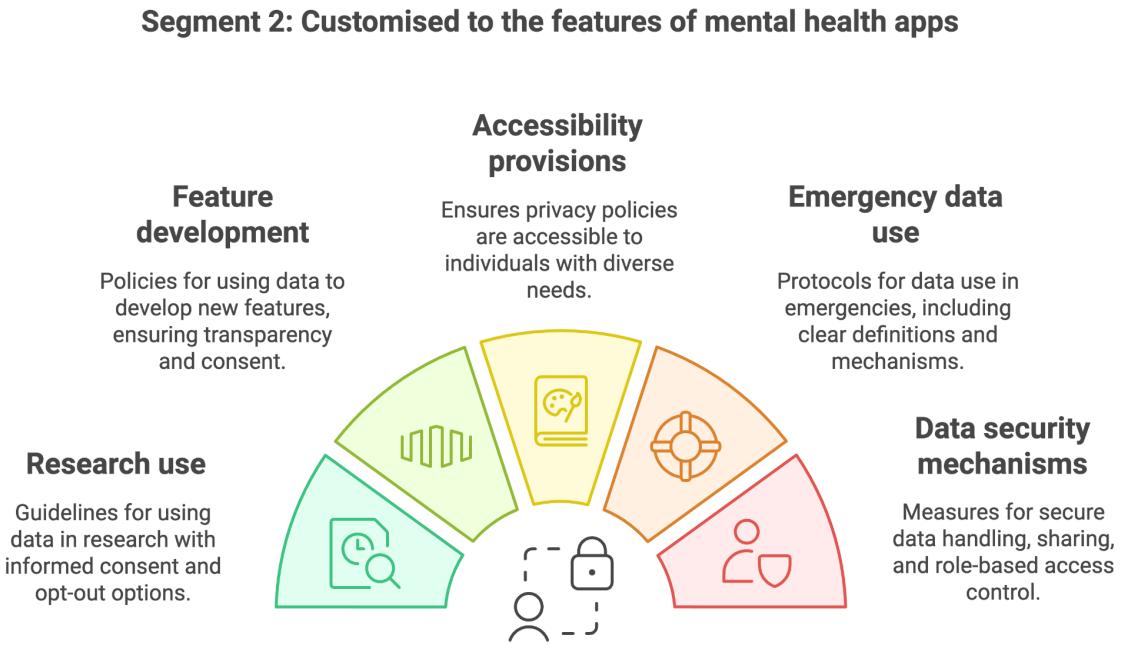
The apps should highlight the user's right to report concerns and dissatisfactions, request resolutions, implement their rights, and provide recommendations about the app. Apps should also inform users of the situations under which they can contact the app and provide the appropriate grievance redressal officer's official position and contact details.

m. *Data protection officer (DPO)*

The policy must clearly outline the appointed data protection officer's details, including their roles and responsibilities.

5.2 Segment 2: Customised features of the mental health apps

Figure 7: Segment 2 –Customised to the key features that mental health apps should include



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

5.2.1 Research use

Individuals must be informed if their data will be used for research purposes. If such consent was implicit in the privacy policy, there should be an option for the person to opt out of the data being used for research, in accordance with the process of purpose limitation. If using the data for research is a new development, the app must obtain consent again, in line with the principle of informed consent, and the privacy policy must be updated to reflect this change.

5.2.2 Use of data for building new features

The privacy policy must specify whether the app intends to use the individual's data to develop new features. It should also clarify whether the analysis will include personal data or anonymised data. Apps must seek consent before using personal data.

a. *Provisions for AI-assisted therapy (if applicable)*

   The privacy policy should inform users if AI is being used to interact with them or record conversations. The policy should also specify the language models used to derive the conversational elements, the extent of data shared, the elements picked up from users' chats to improve their knowledge base, and the sensitivity analysis done on the chats.

b. *Provisions for differences in accessibility needs*

   Individuals with different accessibility needs and neurodivergence may seek mental health support through an app; therefore, the privacy policy should adopt measures to make it accessible and easier to understand. For instance, it could be screen reader-friendly, offer options for different or larger fonts, and use headings and paragraphs to make it easier to read and comprehend.

5.2.3 Use of data in emergency situations

When using a mental health app, situations may arise when app developers need to share information with a legal authority or official. These emergencies could be cases of harm or risk of harm to oneself or others or when a person presses an SOS button (if available in the app). For such instances, the apps need to have in place proper mechanisms to provide support. The policy should clarify what data it will share and with whom, as well as outline

the potential medical or legal intervention. Additionally, the policy should clearly define what constitutes an emergency.

5.2.4 Data use and security mechanisms for mental health features

Mental health apps must provide clear and detailed privacy policies that address data sharing, usage, and security across all interactions. This includes specifying the extent and purpose of information shared with mental health professionals and supervisors for clinical oversight and robust protocols to ensure secure handling and transfer. In peer support communities, the policy must outline how users' shared information is protected, the degree of anonymity or visibility provided, and measures to prevent misuse. Additionally, apps should implement stringent security mechanisms during online interactions, including sessions with professionals and community engagements, while highlighting procedures for secure data storage and sharing with authorised parties. They should establish role-based access control (RBAC) policies, restricting access to sensitive information based on roles and responsibilities, thereby ensuring user trust and transparency.

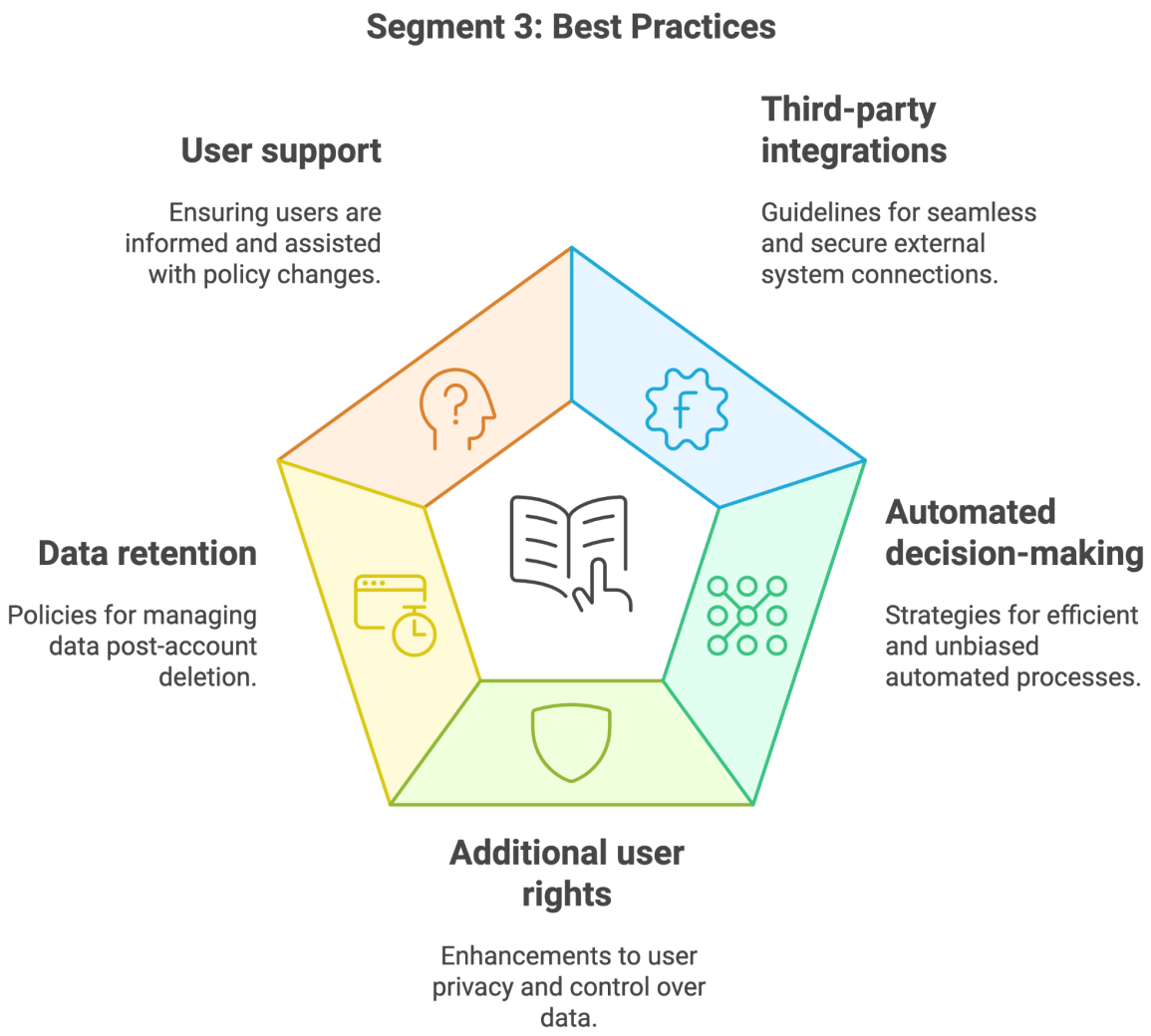
5.2.5 Mandatory data protection impact assessments

While DPIAs are not mandatory, organisations developing mental health apps are encouraged to conduct them, especially as many apps now include AI features such as conversational agents or chatbots. The privacy policy could state the frequency of these assessments.

5.3 Segment 3: Best practices

The best practices observed in international privacy policies that comply with regulations other than the DPDPA serve as guidelines for app developers drafting privacy policies for India's mental health apps.

Figure 8: Segment 3 comprises best practices from privacy policies of international mental health apps



Source: CIS analysis of mental health apps and their privacy policies, May - September 2024.

5.3.1 Specification of third-party integrations

The privacy policy should specify the details of the third-party integrations used within the app and clearly mention the type of organisations and the purpose of the data shared with them.

5.3.2 Automated decision-making

If the mental health app involves specific automated decision-making components, the privacy policy must inform the users of the specific situations that use automated decision-making mechanisms and allow users to opt-out.

5.3.3 Additional user rights

The app should provide users the choice to opt out of the automatic processing of their data, marketing and advertising materials from the app, or when the data is utilised for research purposes. They should also provide users with the option to transfer their data, including data portability.

a. *Data retention for deleted accounts*

   The policy must outline the app's safeguarding mechanism for users who delete their accounts and specify that users have the right to request the deletion of their data when the app's service is terminated.

5.3.4 Discontinuation of the app

The app must specify the security protocols that will continue to protect the data if the app is acquired, shared, or discontinued. The terms of service should clarify that if the app's data is sold, the app will seek the user's consent before sharing or transferring it.

5.3.5 User support for updates to the policy

The policy must specify the processes in place to inform users regarding updates to the privacy policy. The app should inform users through notifications or emails and seek consent if the data is being processed in a way the user had not consented to earlier.

Conclusion

Mental health apps provide help and guidance on mental health issues in a manner that is accessible and allows people to choose the type of interactions they prefer. While these apps advertise a private and secure interface, whether with a chatbot or a therapist, there is a need to look at how private and secure these interactions really are. This study revealed that a few mental health apps in India lack a privacy policy that informs users about data usage upon signing up for these services. While the DPDPA has yet to be implemented, and we still await its Rules, apps dealing with sensitive mental health data should be cognizant of the harm that this data, if used, stored, and shared irresponsibly, could cause. While the DPDPA is not the most stringent legislation in its current form, with health and sensitive personal data removed from the final version, it still details data fiduciary-specific responsibilities. Currently, app developers, including mental health apps, view privacy policies more as compliance requirements than something integral to the accountable provision of health services. As technology develops and the capability of apps to address mental health concerns across different segments is enhanced, ethical considerations, privacy, and trust elements will need to evolve and look beyond mere compliance.

Following a comprehensive review of mental health apps in India, the current report offers a clear and structured framework to guide the development of privacy policies in these apps. By outlining the key aspects that users should be aware of, the framework can help create effective policies that build trust and enhance the effectiveness of privacy policies.

Annexure

List of Indian and international mental health apps analysed

	Name of the App	Country
1.	Wysa	India
2.	Amaha: Mental Health Self-care	India
3.	YourDOST	India
4.	Evolve: Self-care and Meditation	India
5.	manas	India
6.	being: CBT self-care and anxiety	India
7.	Now&Me: Therapy, self-care	India
8.	MindPeers: Therapy and Self-care	India
9.	Mpower: Holistic Mental Health	India
10.	Manoshala	India
11.	CareMe Health -Mental Health	India
12.	The Able Mind	India
13.	mimblu: mental health support	India
14.	TickTalkTo	India
15.	Jumping Minds: Mindful Support	India
16.	IWill: Your Support System	India
17.	THAP: Anxiety, Depression care	India

18.	Kavach: Mental health app for teens	India
19.	Let’s get Happi	India
20.	Felicity: #1 Mental Health App	India
21.	1to1help.net	India
22.	WellM	India
23.	Asmi: Mental Health Counselling	India
24.	Positive Mind Care	India
25.	Mannkaa	India
26.	Rocket Health	India
27.	MindClan	India
28.	PeakMind App	India
29.	Intellect: Create a Better You	International
30.	Sanvello	International
31.	Talkspace	International
32.	BetterHelp	International
33.	Breeze: mental health	International
34.	TalkLife: 24/7 Peer Support	International
35.	Clarity: CBT Self-help journal	International
36.	Bloom: CBT therapy and journal	International
37.	MindDoc: Your companion	International
38.	Youper -CBT therapy chatbot	International

39.	Mindshine: Mental Health Coach	International
40.	Rootd: Panic Attack Relief	International
41.	I Am Sober	International
42.	Elomia: Therapy chat and vent	International
43.	Moodnotes: Mood Tracker	International
44.	Sintelly: CBT therapy chatbot	International
45.	7 Cups: Online Therapy and Chat	International