ISSUE BRIEF | April 2025

Click here for more publications

Delving into Digital Mental Health: Part 2

Relevance of the Digital Personal Data Protection (DPDP) Act in the mental health sector in India

AUTHOR
Elizabeth Mathew

ACKNOWLEDGMENTS
Ramya Pillutla, Tanya Fernandes

Introduction: Data privacy in digital India

The Digital Personal Data Protection Act (DPDP Act)[1] was enacted in August 2023 to govern digital data protection and privacy in India by the Ministry of Electronics and Information Technology. This Act is particularly relevant to the mental health sector with the expanded use of digital means to access mental health support since the COVID-19 pandemic. Whether it is through the state-run National Tele Mental Health Programme (Tele MANAS) initiative, Electronic Health Records used in mental healthcare facilities, or the burgeoning number of digital mental health applications that can be downloaded on mobile phones, the surge in users indicates the increased collection and storage of sensitive mental health data. The use of digital mental health tools and its wide-scale applications in India has been presented in the first brief of this series, Delving into Digital Mental Health: Part 1.

For users accessing digital mental health support services, it is important to understand the legal landscape which protects their data and privacy rights. With the DPDP Act replacing the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) (SPDI) Rules of 2011 as the new data protection law[1], its provisions have direct implications on how personally identifiable mental health information is treated by government agencies, private service providers and researchers. It is critical to note that in the absence of a specific safeguarding framework, confidential data can be hacked, sold or misused by bad actors. This leaves individuals vulnerable to the risks of discrimination, exclusion and exploitation in a socio-cultural context where stigma around mental health is highly prevalent.

In January 2025, the Ministry released the draft Rules for the Act for public comment. The Rules constitute the guiding framework for the implementation of the Act and require extensive consultation before they are finalised.

Through this issue brief, we aim to dissect the DPDP Act, its implications on mental health data, and identify gaps in the Act and the Rules that could compromise its effective implementation in the mental healthcare sector. We highlight the challenges to privacy rights and safety of sensitive mental health data that arise due to existing gaps and propose recommendations to mitigate them.

Background to the DPDP Act

The DPDP Act, 2023, provides safeguards for the processing of digital personal data “in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes”. The Act covers digital data as well as physically recorded data that has been subsequently digitised. It regulates all the aspects of data management such as data collection, access, processing and erasure of data, with the claim of empowering the owner of the data to decide what happens to it once it is shared.

Why is the DPDP Act relevant for mental health?

The National Mental Health Survey conducted by NIMHANS in 2016 reported a staggering treatment gap of 83%, pointing to the large number of people in India who need care but are unable to access it[2]. Digital mental health applications and platforms play a significant role in improving access to support services by removing physical distance and reducing cost of care. But this also translates to an increase in sensitive mental health data in the digital realm.

The mental health sector deals with highly sensitive personal data. This could entail:

- diagnosis and treatment records
- medical histories collected by a mental health facility
- service provider-client sessions data in a clinic
- any personally identifiable mental health data collected by community-based mental health organisations from end-users of their interventions, law enforcement or medical facilities
- any mental health data that is shared through online tests
- data collected by organisations for mental health research.

The prerequisite for an individual to feel safe, trust the judgment of their mental healthcare provider and continue accessing the help they need is the assurance that the information they share about their mental health remains confidential.

Section 23(1) of the Mental Healthcare Act (MHCA), 2017[3], states that "A person with mental illness shall have the right to confidentiality in respect of his mental health, mental healthcare, treatment and physical healthcare", thereby recognising the privacy rights of persons with mental illness.

With the proliferation of digital mental health services to provide accessible and affordable care in the country, thousands of users share their personal data in exchange for services, whether it is with the government, private health facilities or mental healthcare organisations that offer psychosocial support and carry out research. It is also worth noting that the Tele MANAS initiative, which has received more than 19 lakh calls as of March 2025, persists as a main line item under the mental health allocation in the Union Budget 2025-2026[4], indicating the government's continued commitment to expanding digital mental health services in the country.

While digital mental health serves to bridge the mental healthcare treatment gap on one hand, it raises several privacy-related questions on the other: *Who has access to the data? How is its safety being ensured? What happens to the data after the purpose for which it was collected is fulfilled?*

The answers to these questions hinge on the regulatory framework currently governing digital data in the country, the DPDP Act. This warrants an examination of digital mental health data safety and patient privacy through the provisions of the Act.

DPDP Act and international standards for data protection and privacy

The GDPR (General Data Protection Regulation), which is the European Union's legal framework governing data safety and privacy in member countries, is considered a global benchmark for legislation on data governance and privacy. Though the provisions of the DPDP Act find resonance in

Understanding the terms in the DPDP Act

- **Data Principal** – The individual to whom the data belongs or is personally identifiable with.
- **Data Fiduciary** – The entity (individual or group) that determines the purpose and the means of data processing.
- **Data Processor** – The entity contracted by the data fiduciary to process the data.
- **Processing** – Includes collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
- **Access** – The data principal can obtain from the data fiduciary information about what data is being used, how it is being processed and who it is being shared with – whether it is another data fiduciary or the data processors working on the data.
- **Correction** – Having accessed the data under process by the data fiduciary, if the data principal feels that the way the data has been represented should be altered, they can do so.
- **Erasure** – If the data principal wishes to retract their consent and erase the data being processed by the data fiduciary, they can do so. In response, the data fiduciary is required to halt processing and delete all data they had collected for the purpose, regardless of the stage of data processing. The Act emphasises that the data principal must bear the consequences of the purpose not being served owing to the halting of data processing.

the GDPR, it pivots away from it by being more principles-based than prescriptive in its objectives[4].

The following are some of the key principles implicit in the language of the DPDP Act:

- **Purpose limitation** - Refers to restricting use of collected information for the sole purpose for which consent was given. Under the DPDP Act, this principle applies only to consent-based data.
- **Data minimisation** - Refers to restricting the collection of data only to what is relevant for the purpose. This principle, again, only applies to consent-based data under the DPDP Act.
- **Storage limitation** - Regulates the retention of the data once the purpose for which it was collected is fulfilled.
- **Consent for collection and processing of data** - With some exceptions (data that is voluntarily shared, is publicly available or processed for "legitimate purposes"), the data fiduciary can pursue processing only with the consent of the data principal. Consent should be "free, specific, informed, unconditional and unambiguous with a clear affirmative action". The data fiduciary is responsible for issuing a notice informing the data principal (DP) about what data is collected, the purpose for which it is collected and their right to redressal through the Data Protection Board. It specifies that consent should be as easy to withdraw as it was given. The data principal also holds the right to access, correct and erase their data as they choose, though this is confined to consent-based data.
- **Accountability** - Under the DPDP Act, the onus for data protection falls almost entirely on the data fiduciary (DF). The data fiduciary is responsible for ensuring accuracy of information collected if the information

influences decisions concerning the data principal or if it is disclosed to another data fiduciary. The data fiduciary will bear liability if the data processors they contract fail to adhere to data safety protocols.

- **Data integrity and grievance redressal** – The Act requires the data fiduciary to institute appropriate measures to ensure data safety. At the same time, in the event of a breach, the data fiduciary is obligated to inform the data principal about the same. The data principal can approach the Data Protection Board for grievance redressal in the manner communicated via the notice given by the data fiduciary when consent was requested.

Challenges in the application of the DPDP Act in the mental healthcare sector

The lack of a defined category for sensitive personal data

While the SPDI Rules, 2011 drew a distinction between 'personal data' and 'sensitive personal data', the DPDP Act clubs all data regardless of their nature under the umbrella term 'personal data'[1].

Sensitive personal data in the mental healthcare sector, listed in its various forms in the previous section, warrants dedicated and rigorous mechanisms to protect it from being used for illegal and unethical activities, given its very nature and the adverse consequences that could ensue in case of a data breach. This includes discrimination and exploitation of the person with mental illness and incalculable personal distress, compounding their marginalisation and resulting in a loss of trust in mental healthcare institutions.

Although the Act classifies certain DFs as 'Significant Data Fiduciaries' based on the volume and sensitivity of data processed, it does not define what this 'sensitive data' means. The GDPR, for example, delineates the different types of sensitive data such as health, ethnicity and race-related data and provides careful exemptions, especially for health data (Article 9 of the GDPR).

The lack of an explicit mention of sensitive personal data undermines the necessity of separate and tighter standards for procedure for handling confidential mental health data, especially since DFs are expected to institute their own safeguarding mechanisms.

Given the exemption that provisions of the Act are not applicable to data processing for research, archiving or statistical purposes, even though it is only in the case of decisions that do not directly concern the individual, the lack of adequate safeguards puts individually identifiable sensitive personal data at risk of being misused.

To compound this loophole, the Data Protection Board of India may accept a "voluntary undertaking" from the data fiduciary to take action or refrain from taking action in the event of a breach, according to section 32 of the Act. This could protect data fiduciaries from penalties at the expense of privacy rights violations of data principals.

There is also the risk of the redressal process failing to adequately factor in the lived realities of already vulnerable individuals and falling short in delivering proportionate penalties and compensation in case of breaches or misuse. Moreover, the draft Rules impose a fee for appealing in cases where the person is aggrieved by an order or direction of the Board, which impedes equal access to justice.

Recommendations

- Neither the Act nor the draft Rules define 'sensitive personal data' as a distinct category covering physical and mental health data.
- The Rules need to issue detailed guidelines targeting data fiduciaries on processes to ensure data safety and privacy. This should include:
    - classifying data by degree of sensitivity and formulating proportionate security control requirements
    - monitoring through Data Protection Impact Assessments* at stipulated intervals
    - establishing communication protocols with data processors.
- The voluntary undertaking provision must not be permitted in the case of sensitive personal data breach and penalty must be mandated in the Rules.
- The Rules need to spell out graded penalties for varying degrees of violation and factor in socio-economic risks of victims to guide decisions on compensation packages.

Exemptions to start-ups: Sensitive data in the hands of the private sector

As per the Act, any data fiduciary or class of data fiduciaries notified by the state and startups are exempted from:

- providing notice as per section 5(1)** to the DPs
- ensuring that the personal data processed is complete, accurate and consistent
- and affording the DP the right to erase data or withdraw their consent for processing.

This exemption in the Act seems to be geared towards promoting business growth in the country but misses accounting for the fact that a significant proportion of digital mental health service providers in the private sector are classified as startups. India hosts around 446 mental health tech startups which constitutes 6% of the world's total and this is a rapidly growing number. The sector witnessed a remarkable 31% growth in revenue over a single year, from 2023 to the first quarter of 2024[5].

Some of these startups work with members of the LGBTQIA+ community who live with mental health conditions – adding another layer of sensitive personal data, i.e. sexual preferences, that warrants increased safety vigilance[6]. Several instances of commercial sales of sensitive data by businesses are coming to light. Take the case of BetterHelp, an American online counselling service whose users include vulnerable LGBTQIA+ individuals and adolescents. In 2023, the Federal Trade Commission held the company accountable for disclosing sensitive information about the mental health challenges and trackable email addresses of users with third parties including Facebook and Snapchat, compromising user privacy rights[7].

The economic motivation behind this exemption is significantly outweighed by the risks posed by it to individual privacy for large numbers of users who are sharing their personal data based on trust. An exempted mental health startup is more likely to disregard rigorous safety protocols and misuse data for AI-enabled tracking tools that can perpetuate discrimination, or for marketing or selling products for profit.

In another instance of commercialising mental health data, Crisis Text Line, a New York-based mental health start-up operating across countries including the UK and Canada, shared sensitive data of distressed users with a for-profit company to repurpose into customer service software. What's interesting to note here is that the incident brought to light the exclusion of non-profits from the ambit of the US federal consumer protection framework and how this regulatory lacuna coupled with technology rendered service users vulnerable to exploitation[8].

*Data Protection Impact Assessments:
Under clause (c) of Section 10 (2) of the DPDP Act, the Significant Data Fiduciary is required to undertake the DPIA, which is defined as a process comprising:

- a description of the rights of Data Principals
- purpose of the processing of their personal data
- assessment and management of the risk to the rights of the Data Principals, and
- such other matters regarding such process as may be prescribed under DPDP Act.

Recommendations

- Regardless of turnover, organisations that collect and process sensitive mental health data of individuals should operate under strict measures to ensure informed consent, accuracy of information and uphold the Data Principal's right to withdraw consent at any point. It is therefore imperative that the Rules clarify how this exemption to startups will be operationalised and what the safeguards are for data and privacy protection, which is missing in the draft Rules.
- The Rules must clearly define who is a 'significant data fiduciary' and enforce this as a legally binding definition including mental health startups within the ambit. To ensure better compliance, a provision for government support (monetary or technical inputs) in the initial phases could be included to enable set-up for data safeguarding processes.

Exemptions to the government: Concerns around Ayushman Bharat Digital Mission (ABDM) and Tele MANAS

A key critique of the Act is the wide-ranging exemptions granted to the state and its instrumentalities. The law does not cover what exactly encompasses 'instrumentality', but if it is taken to mean any entity that is funded and functions under the mandate of the state, this could include the public healthcare sector and by extension the mental health establishments and programmes it governs – Tele MANAS, eSanjeevani, the District Mental Health Programme, central and state-funded mental health institutions and Ayushman Bharat Health and Wellness Centres (HWCs).

The provisions of the Act are inapplicable if the data is being processed by the state and its instrumentalities for:

1. national security reasons
2. maintenance of public order
3. for research, archiving, and statistical purposes.

Exception 3, listed above, raises particular concern as it seems to imply that not only the government, but businesses as well, can collect and process personally identifiable information for research purposes without the consent or perhaps even the knowledge of the individual.

Ayushman Bharat Digital Mission (ABDM)

ABDM creates a centralised, albeit voluntary, infrastructure for accessing patient data from government and private healthcare institutions. This includes startups that work in the digital healthcare sector, a partnership the National Health Authority actively encourages to bolster innovation and expand reach[9].

Signing up on this digital ecosystem is voluntary and both individuals and private entities can opt out when they choose, which results in all pertinent information being deleted. Nevertheless, it does give rise to questions about who has access to the available data and how health data in general, and mental health data specifically, could potentially be used.

Especially given that digital mental healthcare startups may not require consent from their clients as per the Act, data that is collected by these entities could be further processed and retained by the Ministry of Health and Family Welfare, other instrumentalities and the union government in the form of a centralised repository of readily accessible sensitive health data that could be routed for research purposes, largely without citizen consent.

The draft Rules lay out robust standards governing such exceptional processing conditions in the Second Schedule. This, in large part, mitigates any potential risk of data privacy violation and reflects the influence of the GDPR in its emphasis on the

**Section 5(I) of the DPDP Act:
Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her -
(i) the personal data and the purpose for which the same is proposed to be processed
(ii) the manner in which she may exercise her rights under sub-section (4) of section 6 and section 13
(iii) the manner in which the Data Principal may make a complaint to the Board, in such manner and as may be prescribed.

principle of data minimisation and the rights and freedom of the 'data subject' (Article 89 of the GDPR).

Tele MANAS

Tele MANAS is a state mental health service where individuals voluntarily provide data without explicit consent for the specific purpose of receiving care. As the website states, the data is processed for research, a purpose that stands outside the Act's provisions and hence is excluded from consent requirements for use by government departments.

Although the Tele MANAS website states that patient anonymity and confidentiality will be protected[10], there is little information about how this will be achieved, especially as an RTI revealed that Tele MANAS is yet to have a privacy policy in place[11], putting Tele MANAS users at high risk of privacy violation.

Moreover, the intervention relies on a federated architecture comprising knowledge and tech support partners such as the apex institutions (NIMHANS, IIIT-B, NHSRC), regional coordinating centres and mentoring institutions which will be working closely with the states/UTs to enable successful implementation[12]. This is a soft ground for critical privacy-related questions: How are procedures being regulated? Who is responsible for setting up this regulatory framework? More importantly, what shape will task-sharing take with respect to access, processing and storage of sensitive mental health data? In other words, how is user privacy and data security being operationalised?

Recommendations

- Although the draft Rules define standards for processing non-consent based personal data, it is necessary to stress on additional data security measures for non-consent based sensitive data. This should be rigorously enforced for government entities and businesses alike.
- There is need for a transparent and comprehensive privacy policy for Tele MANAS which clearly lays out access and data sharing controls for the different stakeholders interacting with the information.

Autonomy of persons with mental illness: Can individual privacy rights truly be upheld in proxy?

A major concern is that the Act provides for the joint recognition of a person with disability and their lawful guardian as DP. The law does not delineate provisions to reinstate individual autonomy in instances where the person with disability can act independently or with some degree of support. This highlights the need to understand to what extent a person with mental illness can be adequately represented when it comes to questions about their data privacy, even if it is by someone empowered by the state on their behalf to take decisions in their best interest.

In contrast, under the MHCA, the person with mental illness is presumed to have capacity until proven otherwise. As far as mental healthcare decisions are concerned, the supported decision-making paradigm proposed by the MHCA is anchored in the will and preference of the person with mental illness[13]. It upholds the decisional autonomy of the individual, which the nominated representative and mental health professionals involved in treatment decisions are bound by. This acknowledgement is actioned in the MHCA's provision for advance directives declared by patients seeking care. An advance directive is a document reflecting the care and treatment choices of a patient at a time when they are unable to make informed decisions. Every Mental Health Review Board is required to maintain an online register of advance directives.

In addition to the advance directive, it must be noted that the consideration for supported decision-making in necessary circumstances is contingent on capacity assessment of the patient,

which restricts the opportunities for the nominated representative to stand in for the patient on their treatment and care decisions.

In matters that concern the data privacy rights of individuals with mental illness, it is also pertinent to consider where the jurisdiction of the Data Protection Board instituted under the DPDP Act ends and where that of the Mental Health Review Board set up under the MHCA begins. Although such instances of overlapping jurisdiction could be handled legally on a case-by-case basis, providing protections without clear pathways and mechanisms to claim them when violations occur only serves to annul the purpose of these protections and compound the distress of the person whose rights have been violated.

Recommendations

The draft Rules grant too much power to data fiduciaries to determine the nomination process. It is important that the Rules lay out a detailed protocol that limits the influence of data fiduciaries on this matter. It should also be stipulated that in the event that a person with mental illness loses their ability to make decisions independently and have not nominated anyone to act on their behalf, the process of establishing a nominated representative under the MHCA should take precedence over the DPDPA Rules.

Conclusion

While the DPDP Act is certainly a step in the right direction in data protection legislation in the country, the Act itself and its draft Rules fall short of delineating special considerations for sensitive health data in a rapidly growing digital healthcare ecosystem. This warrants a rethink in convergence with healthcare and lived experience stakeholders for a truly inclusive law that regards the privacy rights and autonomy of the individual.

References

1. Rai, S., & Malhotra, S. (2023, October 31). India is piloting ambitious digital health initiatives while neglecting data safeguards. ScrollIn. https://scroll.in/article/1057716/india-is-piloting-ambitious-digital-health-initiatives-while-neglecting-data-safeguards
2. Gururaj, G. et al. (2016). National Mental Health Survey of India, 2015-16: Prevalence, patterns and outcomes (NIMHANS Publication No. 129). National Institute of Mental Health and Neuro Sciences.
3. India. (2017). Mental Healthcare Act, No. 10, Acts of Parliament, 2017.
4. Amarnani, S. (2025, February 10). Union Budget in Mental Health (2025-26): Key Initiatives & Findings. Indian Counselling Services. Union Budget in Mental Health 2025, ICS, 9999010420
5. Apacible-Bernardo, A., Sonkar, S., & Chakraborty, S. (2023, October). Top 10 operational impacts of India's DPDPA – Comparative analysis with the EU General Data Protection Regulation and other major data privacy laws. The IAPP. https://iapp.org/resources/article/operational-impacts-of-indias-dpdpa-part6/
6. Mukherjee, R. (2024, January 15). Mental healthtech companies see PE funds slip to $3 million in 2023. Times of India. https://timesofindia.indiatimes.com/business/india-business/mental-healthtech-companies-see-pe-funds-slip-to-3million-in-2023/articleshow/106847909.cms
7. Mental health startups make a mark in India's uncharted territory. (2023, October 14). Medical Buyer. https://www.medicalbuyer.co.in/mental-health-startups-make-a-mark-in-indias-uncharted-territory/
8. Bajak, F. (2023, March 3). BetterHelp shared users' sensitive health data, FTC says. AP News. https://apnews.com/article/betterhelp-ftc-health-data-privacy-befca40bb873661d1f8986bb75d8df07
9. Levine, A. (2022, January 28). Suicide hotline shares data with for-profit spinoff, raising ethical questions. Politico. https://www.politico.com/news/2022/01/28/suicide-hotline-silicon-valley-privacy-debates-00002617

References

9. Ministry of Health & Family Welfare, Government of India. (2022, July 28). More than 50 digital health services/ applications integrated with Ayushman Bharat Digital Mission (ABDM)—Within 10 months of its nationwide launch, ABDM has expanded its partners ecosystem to 20 government and 32 private digital health applications [Online post]. PIB Delhi. https://abdm.gov.in:8081/uploads/PIB_1845845_685e874ac3.pdf
10. Ministry of Health & Family Welfare, Government of India. (n.d.). FAQs on the National Tele Mental Health Programme of India. https://telemanas.mohfw.gov.in/faq
11. P K, N. (2023, August 30). Tele MANAS clocks 2 lakh consultations, yet lacks data privacy policy. Deccan Herald. https://www.deccanherald.com/india/tele-manas-clocks-2-lakh-consultations-yet-lacks-data-privacy-policy-2665580
12. Ministry of Health & Family Welfare, Government of India. (2022). Operational Guidelines—The National Tele Mental Health Programme of India.
13. Namboodiri V. (2019). Capacity for mental healthcare decisions under the Mental Healthcare Act. Indian journal of psychiatry, 61(Suppl 4), S676–S679. https://doi.org/10.4103/psychiatry.IndianJPsychiatry_76_19
14. Bondre, A., Pathare, S., & Naslund, J. A. (2021). Protecting Mental Health Data Privacy in India: The Case of Data Linkage With Aadhaar. Global health, science and practice, 9(3), 467–480. https://doi.org/10.9745/GHSP-D-20-00346
15. Watson, E., Fletcher-Watson, S., & Kirkham, E. J. (2023). Views on sharing mental health data for research purposes: qualitative analysis of interviews with people with mental illness. BMC medical ethics, 24(1), 99. https://doi.org/10.1186/s12910-023-00961-6
16. Ali, F., Gajera, G., Gowda, G. S., Srinivasa, P., & Gowda, M. (2019). Consent in current psychiatric practice and research: An Indian perspective. Indian journal of psychiatry, 61(Suppl 4), S667–S675. https://doi.org/10.4103/psychiatry.IndianJPsychiatry_163_19
17. Ahuja, I., & Kapadia, S. (2023, August 22). Digital Personal Data Protection Act, 2023 – A Brief Analysis. Bar and Bench. https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis
18. Chacko, M., Misra, A., & Mishra, S. (2024). Health provider obligations in securing patient information. India Business Law Journal - Law.Asia. https://law.asia/securing-patient-information-2/
19. Geneva: World Health Organization. (2021). Global strategy on digital health 2020-2025. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf
20. Shastri, M., & Mahashur, S. (2023, May 25). Mind Matters: India's Mental Health Budget Crisis. Speaking of Medicine and Health - PLOS Global Public Health. https://speakingofmedicine.plos.org/2023/05/25/mind-matters-indias-mental-health-budget-crisis/
21. Singh, V. (2023, October 3). Indian Startup Spotlight: Innovative Technology Solutions for Mental Health [Online post]. LinkedIn. https://www.linkedin.com/pulse/indian-startup-spotlight-innovative-technology-solutions-vikash-singh?trk=article-ssr-frontend-pulse_more-articles_related-content-card
22. World Economic Forum in collaboration with Deloitte. (2021, April). Global Governance Toolkit for Digital Mental Health: Building Trust in Disruptive Technology for Mental Health. https://www3.weforum.org/docs/WEF_Global_Governance_Toolkit_for_Digital_Mental_Health_2021.pdf
23. India. (2023). Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023. Digital Personal Data Protection Act 2023.pdf (meity.gov.in)
24. Ministry of Electronics & Information Technology, Government of India. (2025, January 3). Draft Digital Personal Data Protection Rules, 2025. Draft Digital Personal Data Protection Rules, 2025 – Innovate India
25. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
26. Mahapatra et al. (2024). Mental health in India: Evolving strategies, initiatives, and prospects. The Lancet Regional Health - Southeast Asia, Volume 20(100300). https://www.thelancet.com/journals/lansea/article/PIIS2772-3682(23)00160-9/fulltext