RESEARCH PAPER

Data Privacy and Confidentiality in Mental Healthcare in India: An Integrated Governance Framework under the Mental Healthcare Act, 2017 and the Digital Personal Data Protection Act, 2023

Sharma S[1*], Vashishth A[2]
[1*]Ph.D. Scholar, School of Law, Sushant University, Gurugram, Haryana, India
Email: sudeepsharma0025@gmail.com
[2]Associate Professor, School of Law, Sushant University, Gurugram, Haryana, India

Received: 15th Jul, 2026 | Revised: 25th Jul, 2026 | Accepted: 5th Aug, 2026 | Available Online: 12th Aug, 2026

Abstract
India's mental healthcare framework is undergoing rapid change under the pressure of digitization; however, the governing legal framework on confidentiality of mental health records has evolved more slowly. This raises an important question: whether the Mental Healthcare Act, 2017 (the "MHA, 2017") and the Digital Personal Data Protection Act, 2023 (the "DPDP Act, 2023"), together with the Digital Personal Data Protection Rules, 2025 (the "DPDP Rules, 2025"), provide a suitable legal framework for protecting psychiatric records? The provisions of confidentiality under MHA, 2017 are examined in conjunction with the DPDP Act, 2023, with reference to the constitutional right to privacy recognized in *Justice K.S. Puttaswamy (Retd) v Union of India*. The removal of a separate category concerning the sensitive personal data under the DPDP Act, 2023, its failure to engage with the MHA, 2017's capacity-based approach to fluctuating decision-making ability, and the breadth of the statutory exemption available to the Government collectively result in psychiatric information and mental health data not receiving automatic category-based enhanced protection under the general data protection statute, raising questions as to whether the combined framework provides safeguards proportionate to the risks associated with such information.
Drawing exclusively upon Indian constitutional doctrine and the governing statutory framework under MHA 2017 and the DPDP Act 2023, this article discusses that, although each framework is broadly coherent when viewed independently; their interaction may produce overlapping consent requirements where both statutory consent frameworks apply, an exemption power lacking a dedicated mechanism of prior independent oversight, and an enforcement mechanism whose institutional independence raises legitimate concerns where executive action itself is in issue. Addressing these shortcomings requires legislative reforms and brings mental health data protection into closer conformity with the constitutional standard of proportionality.

Keywords: Mental Healthcare Act, 2017; Digital Personal Data Protection Act, 2023; Data Privacy; Confidentiality; Constitutional Privacy
How to cite this article: Sharma S1* Vashishth A2. Data Privacy and Confidentiality in Mental Healthcare in India: An Integrated Governance Framework under the Mental Healthcare Act, 2017 and the Digital Personal Data Protection Act, 2023. Int J Drug Deliv Technol. 2026;16(76s):2037-2046. DOI: 10.25258/ijddt.16.76s.196.

1. Introduction

In India, discussions around mental illness get influenced more by stigma and social cover-up instead of questions of legal rights and protections available to persons who have mental illness. Families have often hidden a diagnosis to protect marriage prospects, jobs, and social reputation within the community, while confidentiality historically operated through professional ethical obligations and general legal principles instead of the express mental-health-specific statutory right subsequently created by the MHA, 2017.[1]

The MHA, 2017 placed the confidentiality of mental health information on an express statutory footing by recognizing it as a right of persons with mental illness.[2] It came into force at a moment when Indian healthcare was beginning to undergo rapid digital transformation. This process has since accelerated through electronic health records and government-led digital health initiatives.[3] Six years later, the enactment of the DPDP Act, 2023 provided a general statutory framework for the protection and lawful processing of individuals' digital personal data against the backdrop of the right to privacy under Constitution. The Act, however, provided a framework for the general application of data privacy rather than one designed specifically for psychiatric records. Whether these two statutes, read together and in view of the constitutional privacy jurisprudence, adequately protect the confidentiality of mental health records remains an important unresolved question. The complexity does not arise because either statute is fundamentally defective when viewed in isolation; rather, it emerges from the way the two statutory frameworks interact with respect to the confidentiality of psychiatric records and data.

The MHA, 2017 confers a statutory right to confidentiality on a person's mental health, treatment, mental healthcare and physical healthcare, but it does not create a confidentiality-specific offence or a dedicated compensatory remedy for breach of that right, although section 108 contains a general penalty for contravention of provisions of the Act or rules or regulations made thereunder.[2,4] The DPDP Act, 2023 governs the same information where it falls within the Act's application to digital personal data but, unlike the earlier Data Protection Bill of 2019, does not classify health data as a distinct category warranting enhanced statutory protection, reflecting the legislative shift in the framework ultimately enacted.[5] Read together, the two statutes create overlapping and, at times, insufficiently coordinated obligations within the same clinical or therapeutic relationship, without providing an express framework for their reconciliation. The result is legal uncertainty rooted in the statutory design itself rather than solely in how these two statutes are implemented on the ground.

The consequences of these overlaps are not merely theoretical; they affect the day-to-day handling, disclosure, retention, and erasure of mental health records. The consequences of unauthorised or adverse disclosure of sensitive medical information are illustrated by *Mr X v Hospital Z*, where disclosure of the patient's HIV-positive status resulted in the cancellation of his proposed marriage;[6] it can also surface in matrimonial proceedings under the Hindu Marriage Act, 1955[7]. Further, on one widely reported occasion, after the patient's death, the diagnosis and treatment-related data got circulated in the public domain, through disclosure made by the patient's own doctor.[8]

In India, the costs of revealing a person's mental health standing are not limited only to embarrassment; historically, various statutory regimes have attached legal consequences to mental illness or to the distinct legal concept of 'unsoundness of mind', with implications for employment, political participation, marriage and the exercise of legal capacity. Disclosure of psychiatric information may thus expose an individual to stigma or disadvantage, notwithstanding that the disclosure does not itself result in any statutory incapacity or disqualification.[1] Data protection, for persons living with mental illness, is therefore not a matter of regulatory compliance alone but bears directly upon the dignity, autonomy, social standing and equal treatment that the MHA, 2017 seeks to secure.

The scope of this article is confined to Indian constitutional doctrine on privacy and the two statutes directly governing mental health data, namely the MHA, 2017 and the DPDP Act, 2023, read together with the DPDP Rules notified in 2025. Comparative data protection regimes are not considered. The analysis draws exclusively upon the constitutional privacy jurisprudence beginning with *Puttaswamy*, the relevant statutory provisions, and Indian legal and clinical literature examining their operation, cited throughout.

2. Materials and Methods

This article adopts a doctrinal legal research methodology, undertaking a textual and purposive analysis of the MHA, 2017, the DPDP Act, 2023 and the DPDP Rules, read against the constitutional privacy jurisprudence originating in *Justice K.S. Puttaswamy (Retd) v Union of India*[13].

Primary sources consist of the Constitution of India, the two governing statutes and subordinate rules identified above, and reported judgments of the Supreme Court of India bearing on informational and medical privacy. Secondary sources consist of peer-reviewed articles and commentary examining the operation and implementation of the MHA, 2017 and the DPDP Act, 2023 in the specific context of mental healthcare, identified through a targeted review of Indian legal and clinical periodicals.

As noted above, the scope is limited to Indian constitutional doctrine and the two statutes directly governing mental health data; comparative regimes fall outside it. Statutory text and judicial reasoning are examined against the proportionality standard set out in Puttaswamy[13], and the resulting gaps form the basis for the legislative and institutional recommendations set out in Part 3.5.

3. Results and Discussion

3.1 The Constitutional Foundations of Informational Privacy

3.1.1 From Kharak Singh to Puttaswamy

For over half a century, Indian courts struggled to agree on whether the Constitution protected privacy at all. In *MP Sharma v Satish Chandra,* an eight-judge bench was subsequently understood in *Puttaswamy* as having rejected the subsistence of a general privacy right under the Constitution in the context before it. In *Kharak Singh v State of UP,* the majority had a similar conclusion, despite the influential dissent of Subba Rao J, who interpreted the guarantee of personal liberty in Article 21 as encompassing freedom from encroachments on private life.[9,10] *In Gobind State of Madhya Pradesh, the Supreme Court took a step toward recognizing a qualified right to privacy as a penumbral freedom, albeit without* conclusively identifying its constitutional foundation.[11] The decision in *People's Union for Civil Liberties v Union of India* marked a further development by holding that unchecked telephone surveillance violated both Article 21 and implicated the freedoms guaranteed under Article 19.[12]

The constitutional uncertainty that was created by these decisions was ultimately resolved in 2017, when a nine-judge bench unanimously held in

Justice K.S. Puttaswamy (Retd) v Union of India that privacy is intrinsic to Article 21 and forms part of the broader guarantees contained in Part III of the Constitution.[13] In the plurality opinion, Justice Chandrachud recognized informational privacy as a distinct facet of that right and emphasized the necessity for a comprehensive data protection statute.[13]

The judgment also articulated the constitutional standards that have since guided various matters of judicial review concerning privacy restrictions. Any measure restricting privacy must be backed by law and must pursue a legitimate State aim through means satisfying the constitutional requirements of necessity and proportionality.[13] This analysis of the confidentiality exceptions in the MHA, 2017 and exclusions in the DPDP Act, 2023 is based on that proportionality framework. The Court revisited these principles extensively in 2018 in the Aadhaar litigation. Although the constitutional validity of the core scheme was upheld, its extension to private authentication was invalidated.[14] The Aadhaar decision further demonstrates that different components and applications of a statutory data-processing framework must independently withstand constitutional scrutiny, including the requirements of necessity and proportionality.

3.1.2 Mr X v Hospital Z and the Qualified Nature of Medical Confidentiality

Nearly two decades before *Puttaswamy*, the Supreme Court had considered the broader scope of medical confidentiality in India. In *Mr X v Hospital Z*, a hospital disclosed a patient's HIV status to his prospective in-laws, following which the proposed marriage was called off.[6] Although the Supreme Court recognized that the patient enjoys a right to medical confidentiality, it held that the said right is not absolute. The Court emphasized that disclosure could be justified where withholding the information would expose the prospective spouse to the risk associated with the patient's HIV-positive status.[6] That reasoning provided in *Mr X v Hospital Z* is reflected in, or is at least consistent with, the harm-prevention and threat-to-life exceptions which were afterward incorporated into section 23(2) of the MHA, 2017. Indian law has therefore long recognized medical confidentiality as an important legal right of an individual, but qualified, not absolute, when competing public interests or the rights and safety of identifiable third parties justify disclosure. Its protection depends upon a careful balancing of individual privacy and confidentiality against competing public and private interests, rather than upon an inflexible rule of absolute non-disclosure.

3.1.3 The Distinctive Stakes of Mental Health Data

Puttaswamy and *Mr X v Hospital Z* establish the constitutional and judicial foundations of medical confidentiality, yet mental health data is not simply medical data carrying a different diagnostic code. Its distinctive character becomes evident for two principal reasons. The first is stigma, where the risk of disclosure is compounded by enduring societal approaches towards mental illness, altering how a person is perceived within the family, workplace, and wider community long after any acute episode has passed.[1] The second lies in the historical association of "unsoundness of mind" with legal incapacity or disqualification in matters such as voting, marriage, and testamentary capacity under various statutory provisions. Consequently, disclosure may expose an individual to significant stigma and social disadvantage, while legal incapacity or disqualification depends upon the conditions prescribed by the particular law rather than upon disclosure alone.[1] A main purpose of enacting the MHA, 2017 was to move away from status-based assumptions of incapacity. Therefore, Section 4 of the MHA, 2017 adopts a functional test of capacity for mental healthcare and treatment decisions, while Section 14(9) expressly recognizes the capacity of individuals with mental illness, who may require varying and different levels of support from their nominated representatives.[2]

3.2 The Statutory Architecture: Confidentiality under the MHA, 2017

3.2.1 The Right to Confidentiality and Its Exceptions

The MHA, 2017 recognizes confidentiality as a statutory right. Section 23(1) guarantees the right to confidentiality in respect of his or her treatment, mental healthcare, mental health, and physical healthcare. Section 23(2) qualifies that right by prescribing the limited circumstances in which health professionals providing care or treatment may disclose such information.[2] The statutory protection extends beyond conventional medical records.

Section 24(1) further prohibits a photograph or other information relating to a person undergoing treatment at a mental health establishment from being released to the media without the consent required under that provision. The practical significance of this protection was starkly illustrated in 2020, when the late actor Sushant Singh Rajput's therapist publicly disclosed details concerning his psychological condition during a media interview. The incident demonstrated that breaches of psychiatric confidentiality are not confined to institutional data failures and may equally result from disclosures by the very professionals to whom patients entrust their most sensitive information.[2,8]

The statutory assurance regarding confidentiality under MHA, 2017 is not absolute. Section 23(2) permits disclosure in specified circumstances, including disclosure to the nominated representative inlcuding other treating professionals, where necessary to prevent harm to a third party or a threat to life, pursuant to an order passed by the concerned Mental Health Review Board, Central Authority,

High Court, Supreme Court or another competent statutory authority, or in the interests of "public safety and security".[2] Although the latter exceptions broadly reflect the approach adopted in the Supreme Court's decision in Mr X v Hospital Z, the Act offers little procedural guidance governing their exercise. In particular, there is no requirement for the reasons of disclosure to be recorded, nor does it prescribe requirements of prior authorization, while it also does not define "public safety". Therefore, considerable discretion lies with the treating professional, without any express mechanism within Section 23 itself for independent oversight or a process of review.

3.2.2 The Enforcement Gap

The MHA, 2017, while establishing confidentiality as a legislative right, does not create a confidentiality-specific offense or a dedicated statutory compensatory mechanism for an unauthorized disclosure. Section 108 nevertheless provides a general punishment for contravention of the Act's provisions or the rules or regulations made under it and is therefore relevant to a contravention of section 23. The enforcement gap is consequently not the complete absence of a statutory penal provision, but the absence of a bespoke remedial and enforcement framework specifically directed at breaches of mental health confidentiality.[2] Duffy and Kelly identified related limitations in the confidentiality framework in their assessment of the Mental Healthcare Bill, 2016 against the World Health Organization's Resource Book checklist on Mental Health, Human Rights and Legislation. Their assessment found that, although the Bill recognized confidentiality and provided circumstances in which disclosure was permissible, it satisfied only five of the eleven relevant checklist criteria (45.4 percent). Most notably, it did not meet the requirement that breaches of confidentiality should attract specific legal consequences.[4] Consequently, an individual whose mental health information is disclosed in violation of section 23 of the MHA, 2017, does not have the benefit of a dedicated statutory compensation or confidentiality-specific remedial procedure within the MHA itself, notwithstanding the possible recourse to its general contravention provision in section 108 or to other remedies available under law.

3.2.3 The Unresolved Family and Carer Question

A further source of uncertainty lies in the legal position of family members and carers under the MHA, 2017, because the nominated representative, who could be a family member but need not be, is entrusted with significant statutory responsibilities. That representative may be privy to information that is released under section 23(2)(a) for the proper discharge of those statutory functions.[2] The Act, however, stops short of conferring an independent right upon family members or carers to access a person's mental health information solely by virtue of their relationship with the patient. In the absence of being appointed as the nominated representative or the patient's consent, the MHA confers no such entitlement solely by reason of the familial or caregiving relationship, subject to the other statutory grounds permitting disclosure.

Duffy and Kelly identify this as a significant point of divergence from the World Health Organization's *Resource Book on Mental Health, Human Rights and Legislation*, which adopts a broader approach to information-sharing with carers. Simultaneously, they observe that the UN Convention on the Rights of Persons with Disabilities ("UNCRPD"), which the MHA, 2017 was enacted to give effect to, contains no comparable requirement to recognize independent informational rights for carers.[4] The legislative approach is therefore consistent with the broader normative framework of the UNCRPD, which places individual autonomy at the center of decision-making and prescribes that people having mental illness are the rights holders rather than passive recipients of family care.[1],

3.3 The DPDP Act, 2023 and Rules, 2025

3.3.1 The Disappearance of "Sensitive Personal Data"

The long title to the DPDP Act, 2023 recognizes both aspects, i.e., the right of individuals to safeguard their personal data as well as the need to process such data for lawful purposes. The Act was enacted against the constitutional backdrop of informational privacy recognized in *Puttaswamy*, although the statutory text does not itself declare that it implements that judgment.[15] The legislative position was not always the same. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, framed under the Information Technology Act, 2000[16], defined a separate category of "sensitive personal data or information" to include physical, psychological, and mental health conditions and medical records and history, and imposed specific requirements governing the collection and disclosure of such information.[17,18] The distinction was also preserved in earlier iterations of India's proposed data protection legislation, including the 2019 Bill, which recognized sensitive personal data as a category distinct from ordinary personal data. That distinction, however, was omitted from the final legislation ultimately enacted in 2023 as the DPDP Act. 2023.[19] As enacted, the DPDP Act, 2023 adopts a single, generic definition of personal data. It does not provide automatic category-based enhanced statutory protection for health, mental health, or biometric information as distinct categories of personal data.

Consequently, an organization processing psychiatric information and data is generally governed by the same general statutory obligations as any other data fiduciary unless it is classified as a

Significant Data Fiduciary under section 10. That designation depends upon an assessment of statutory factors that expressly include both the volume and sensitivity of the personal data being processed, threat to the rights of the Data Principals, and specified public-interest considerations.[15,20] The current framework under the DPDP Act, 2023, makes no meaningful distinction between psychiatric information and routine classifications of personal data. From the proportionality principles articulated in *Puttaswamy*, this represents a significant shift away from a risk-based approach to informational privacy.

3.3.2 Consent, Capacity and the Double Consent Burden

The DPDP Act, 2023 has a consent-centric regime for personal data processing but allows processing without consent in the "certain legitimate uses" specified in section 7. Section 6 requires consent to be specific, free, informed, unconditional and unambiguous. In contrast, Section 9 prescribes additional requirements for processing the data of children and persons with disabilities, where the person with disability has a lawful guardian.[15] Significantly, however, Section 9 contains no cross-reference to the capacity framework established under the MHA, 2017. Instead, it requires the lawful guardian's verifiable consent for processing the personal data of a person with disability, whose guardian has been appointed as per the provisions of the Act. The DPDP framework does not expressly reconcile this mechanism with sections 4 and 14(9) of the MHA, 2017, which adopt a functional and support-oriented approach to mental healthcare decision-making. Section 81 of the MHA performs a different function: it provides for preparation of guidance concerning assessment of capacity.[2,21] In the context of mental health care practice, Sethi and colleagues describe the practical consequence as a "double consent burden". Mental health professionals must first obtain consent for treatment under the MHA, 2017. Where the associated processing of personal data relies upon consent under the DPDP Act, they must also satisfy that separate statutory consent regime under the MHA, 2017. The legislation provides no express mental-health-specific method for reconciling these two parallel statutory requirements, where both consent frameworks apply.[19] The difficulty becomes particularly acute where an individual's decision-making capacity fluctuates over time, a possibility that the consent framework under the DPDP Act, 2023 neither expressly addresses nor provides any mental-health-specific mechanism to accommodate. A similar concern is evident in the Health Data Management Policy prepared under the Ayushman Bharat Digital Mission. The National Health Authority first issued the Health Data Management Policy in 2020, with subsequent proposals for revision forming part of the evolving ABDM privacy framework. The Policy permits a nominee to provide consent where an individual is "mentally incapacitated", yet it neither defines that expression, nor prescribes a clinically integrated procedure for assessing the individual's decision-making capacity. The Policy likewise contains no cross-reference to the capacity framework under Section 4, read with Section 19(9) of the MHA, 2017, which reflects the broader lack of coordination between India's mental health and digital health governance frameworks.[1] To address these difficulties, Sethi and colleagues advocate a layered consent framework under which patients could make separate and granular decisions regarding clinical treatment and the processing as well as handling of their personal data. The DPDP Act does not prohibit purpose-specific or granular consent; the gap lies instead in its failure to provide a specialized framework coordinating data-processing consent with treatment consent and fluctuating mental healthcare decision-making capacity.[19]

3.3.3 The Government Exemption Power

The DPDP Act, 2023 recognizes several situations in which the personal data may be handled and processed without consent. Section 7(b), for example, permits such processing in specified circumstances connected with the State providing or issuing a subsidy, benefit, service, certificate, license or permit, subject to the conditions laid down in that provision. In addition, section 17(2) empowers the Central Government, by notification, to exempt the instrumentality of the State from the application of specified provisions of the Act on grounds including State's sovereignty, security, public order and the prevention of cognizable offenses.[15] Section 17(2) has attracted academic criticism in light of the constitutional principles articulated in *Puttaswamy*. Under the proportionality framework established in that decision, any statutory restriction upon any fundamental right must be supported by law and defined with sufficient precision to satisfy the test of legality. The breadth of section 17(2), in absence of a dedicated statutory mechanism of prior independent authorization or oversight, therefore, raises a legitimate question as to whether particular exemption measures affecting highly sensitive information would satisfy those constitutional requirements. Such notifications nevertheless remain subject to constitutional judicial review.[5] In practical terms, under Section 7(b) of the DPDP Act, 2023, an applicant's personal data, including psychiatric information, may in the circumstances specifically prescribed by that provision be processed by the State without reliance on the consent being the legal base for processing. Due to this, the processing entity also benefits from an exemption granted under Section 17(2), certain statutory obligations and corresponding rights of the individual may cease to apply, thereby limiting the individual's ability to know that such processing has

occurred or to challenge it through the ordinary mechanisms under the Act. This outcome may require scrutiny against the constitutional commitment to transparency, accountability and informational privacy that the Supreme Court in *Puttaswamy* articulated.

3.3.4 The Data Protection Rules 2025: A Sector-Blind Design

Following an extended period of legislative uncertainty, the DPDP Rules, 2025 were notified in 2025, together with the establishment of the Data Protection Board of India and a staggered commencement framework under which different provisions of the Act and Rules become operative at different stages.[22,23] The Rules provide important operational guidance for implementing the DPDP Act, 2023. DPDP Rule 3 prescribes the content of privacy notices, Rule 6 prescribes minimum reasonable security safeguards, including specified organizational and technical protective measures, Rule 13 prescribes additional obligations applicable to Significant Data Fiduciaries, including the prescribed framework relating to data protection audit and impact assessments, and the First Schedule prescribes detailed obligations applicable to Consent Managers.[20]

Despite these additions, the regulatory framework does not classify mental health information as a separate category of personal data. In particular, the obligation to conduct impact assessments applies only to entities recognized and classified as Significant Data Fiduciaries. Although section 10 expressly includes both volume and sensitivity of the personal data, together with risk to Data Principals, among the factors relevant to such designation, a small organization handling highly sensitive psychiatric data may nevertheless remain outside the enhanced obligations unless it or its class is designated as a Significant Data Fiduciary. In contrast, a substantially larger organization processing comparatively fewer sensitive data may be subject to it **if** designated under section 10.[15,20] The Rules therefore strengthen the operational framework established under the DPDP Act, 2023 without creating an automatic enhanced regulatory category for mental health information. The resulting concern is therefore the absence of category-specific safeguards triggered by the nature of psychiatric data itself, not that the statute entirely fails to take account of sensitivity or risk.[20]

3.4 Where the Two Regimes Meet: Compound Gaps

3.4.1 Fragmented Governance of Mental Health Data

Although the MHA, 2017, together with the DPDP Act, 2023, now regulate the same category of data where circumstances fall within their respective scopes, they were enacted at different times, pursue different legislative objectives, and operate through distinct regulatory frameworks. Neither statute provides an express mechanism for coordinating or reconciling their respective requirements where both statutes apply to the same category of personal data, including psychiatric records. This lack of coordination is evident in the treatment of statutory disclosure obligations. Section 23(2) of the MHA, 2017 provides for certain exceptions to the general duty of confidentiality where the mental health information can be disclosed under certain circumstances, like where such disclosure is needed to avert the risk and threat to life, to protect a person from harm or violence, or for the interest of public safety and security. The DPDP Act, 2023, however, contains its own grounds and basis for processing personal data, including the "certain legitimate uses" under section 7, but does not specifically map those grounds onto the disclosure exceptions contained in section 23(2) of the MHA, 2017. A treating professional relying upon an exception contained in the MHA, 2017 is, therefore, left without an express cross-statutory rule identifying how that disclosure should be characterized under the DPDP framework. A similar lack of coordination is evident under the DPDP Rules, 2025. While the Rules require certain data fiduciaries to undertake annual impact assessments, they contain no provision for coordinating with or recognizing the supervisory role already exercised by the State Mental Health Authorities over mental health establishments within their statutory jurisdiction. These examples illustrate a broader structural problem between the two statutory regimes that regulate the same underlying clinical information but do so without a reciprocal framework for assessing risk or any institutional machinery for coordinating their respective obligations. The resulting fragmentation is not merely administrative; it reflects the lack of an integrated legislative approach to the governance of mental health data.

3.4.2 A Consent Architecture That Cannot See the Patient It Was Built For

A more fundamental inconsistency becomes apparent when the consent frameworks established by the MHA, 2017 and the DPDP Act, 2023 are examined together instead of in isolation. Read together, Sections 4 and 14(9) of the MHA, 2017, informed by the principles embodied in the United Nations Convention concerning the Rights of Persons with Disabilities, adopt a functional and support-oriented approach to mental healthcare decision-making. Section 81 supplements that framework by requiring the preparation of guidance concerning assessment of capacity rather than itself creating the presumption of capacity and emphasizing supported decision-making wherever required.[2,24] By contrast, section 9 of the DPDP Act, 2023 makes no reference to that framework. It requires verifiable guardian consent specifically where the data impacts a person with disability, who has a legal guardian, and the "double consent

burden" identified by Sethi and colleagues is therefore more than an administrative complication, where both treatment consent and data-processing consent are independently required.[19] The practical consequences and outcome are particularly evident for persons whom the MHA, 2017 seeks to protect. A patient whose decision-making capacity fluctuates during treatment may have to comply with two separate consent regimes that operate in the absence of any statutory mechanism for coordination. The MHA, 2017 proceeds through its functional capacity and supported decision-making framework, with support provided wherever required, whereas the DPDP Act, 2023 regime does not specifically integrate its lawful-guardian provisions with that framework and does not expressly accommodate fluctuating decision-making capacity. The resulting difficulty extends beyond administrative complexity. It reflects an unresolved interface between a mental-health-specific model of functional capacity and support and a general data-protection regime that recognizes lawful guardianship without expressly integrating the MHA framework.

3.4.3 Institutional Dependence and Regulatory Oversight under the DPDP Act, 2023

The creation of the India's Data Protection Board by the Government appears to fill the enforcement gap under the DPDP Act, 2023; however, its institutional design has generated legitimate questions concerning institutional independence. Section 19 of the Act provides for the appointment of the Chairperson and other Members of the Board by the executive and sets out broad eligibility criteria for such appointments. Section 20 stipulates a two-year term, with the possibility of re-appointment. However, the short renewable term and the significant role played by the Central Government throughout the appointment process raise questions about the institutional independence of the Board's functioning.[5,15,25] These institutional features assume particular significance because the same legislation confers upon the Central Government the broad exemption power. A regulatory body whose chairperson and members are appointed through an executive-controlled process for relatively short renewable terms may raise legitimate concerns regarding institutional independence when called upon to scrutinize the legality or consequences of executive decisions falling within its statutory jurisdiction**.**

There is no statutory mechanism that requires the Data Protection Board to coordinate with the Mental Health Review Boards set up under the MHA, 2017, and this absence has real consequences for patients. Consequently, if someone's mental health data has been disclosed unlawfully, they may face fragmented remedial pathways depending upon the particular statutory violation alleged. The Data Protection Board can determine whether the processing breached the DPDP Act, 2023; however, it cannot exercise general jurisdiction under the MHA, 2017. Conversely, Mental Health Review Boards exercise only those powers and functions conferred upon them by the MHA, 2017 and should not be treated as possessing plenary jurisdiction over every breach of the Act, including every alleged breach of confidentiality, unless a specific statutory basis exists. The result is not purely an oversight, but two parallel enforcement regimes that trace the same issue; however, they never intersect, and the architecture ends up entrenching the very fragmentation it should have resolved.

3.4.4 The Residual Surveillance Risk

Considered individually, the concerns identified in Parts 3.3.3 and 3.4.3 are significant. Read together, however, they reveal a broader structural risk. The combined outcome of the exemptions contained in sections 7(b) and 17(2) of the DPDP Act, 2023, the institutional limitations of the Data Protection Board, and India's historical association of mental illness with legal incapacity and disqualification under various statutory regimes creates a risk that extends beyond the concerns ordinarily associated with the processing of commercial personal data.

On paper, at least, a welfare or security program that processes psychiatric information is subject to the same accountability regulations as any other government data processing activity. But when governance fails here, the bets are often higher than they would be for regular personal data. Much of India's legal history has used mental disease, or "unsoundness of mind", as a basis for legal incapacity and disqualification under one legislation after another. The stigma connected to psychiatric illness rarely stops when therapy does; it tends to outlast the sickness itself. And this is exactly where the proportionality framework from *Puttaswamy* comes into play. A limitation of informational privacy can be compatible with constitutional requirements only if the protections are appropriate to the legitimate aim sought and take proper account of the nature and effects of the information concerned. Those dangers are specific to psychiatric data. The combination of the MHA with the existing DPDP framework does not yet have sufficient built-in safeguards to manage those unique risks.

3.5 Recommendations

The analysis in Parts 3.2, 3.3 and 3.4 demonstrates that the principal weaknesses in the existing framework arise not from either the MHA, 2017 or the DPDP Act, 2023 viewed independently, but from the absence of any coherent mechanism for coordinating the two where both govern the same category of mental health information. Correction of these flaws demands legislative and institutional reform proceeding on the basis that the two frameworks constitute a single system, and not merely amendment of one Act while the other is left untouched. The reforms proposed in what follows

are addressed to the structural weaknesses already identified, with a view to strengthening the protection afforded to mental health information without disturbing the underlying purposes of either statute.

3.5.1 A Statutory Mental Health Data Protection Code

Parliament should enact a dedicated framework governing mental health data, restoring in substance the more stringent protections that were formerly available for sensitive personal data. At the very least, such a framework would require data protection impact assessments to be undertaken by every fiduciary handling mental health data, irrespective of the size of the entity concerned. A five-person clinic and a five-hundred-bed hospital deal in mental health information of equal sensitivity, and the compliance obligation imposed should accordingly be calibrated to the risk the data presents rather than to the scale of the entity holding it. The difficulty at present is that the DPDP Act, 2023 and the MHA, 2017 were each drafted without reference to the other, so that neither statute contains any mechanism for reconciling the requirements of the second. Nor can delegated legislation supply the remedy: rules framed under one Act possess no authority to alter or override obligations imposed under a separate Act. What the gap calls for, in consequence, is either a standalone legislative instrument or coordinated amendment of both statutes at once.

3.5.2 A Capacity-Based Supported Consent Framework

The DPDP Rules should be amended to incorporate an express cross-reference to the capacity framework contained in section 4, read with section 14(9), of the MHA, 2017 and, where relevant, the capacity-assessment guidance contemplated by section 81. The regulatory framework should further distinguish consent to clinical treatment from consent to the processing of personal data, though both may be assessed through a single, clinically informed determination of decision-making capacity. Such a requirement will inevitably add to the administrative burden already carried by treating institutions and healthcare facilities, particularly where a patient's capacity is not static but fluctuates over the course of treatment, necessitating reassessment rather than a one-time determination at intake. That burden is properly attributed to the clinical realities of mental healthcare rather than to any deficiency in the proposed framework. It bears noting, in any case, that the present position is scarcely less onerous: patients and clinicians must already navigate two entirely separate statutory requirements, one governing treatment consent and the other governing consent to data processing, with the MHA, 2017 and the DPDP Act, 2023 offering no mechanism by which the two might be reconciled.

3.5.3 Specific Penalties for Breach of MHA Sections 23 and 24

Chapter XV of the MHA, 2017 should to be amended to provide a dedicated remedial framework for breaches of confidentiality, incorporating civil, penal and regulatory consequences proportionate to the unauthorised disclosure of confidential information protected under sections 23 and 24. It may be observed that section 108 already prescribes a general penalty for contravention of the Act; this, however, is not equivalent to a provision addressed specifically to breaches of mental health confidentiality, and its generality leaves considerable uncertainty as to the scope and enforceability of the protection sections 23 and 24 are meant to secure. A dedicated provision would remove much of that uncertainty. Existing statutory exceptions permitting disclosure may remain unaffected. Such an amendment would address the absence of a bespoke enforcement mechanism and strengthen the practical enforceability of the statutory right to confidentiality.

3.5.4 Statutory Independence for the Data Protection Board

The institutional independence of the Data Protection Board should be strengthened through appropriate amendments to section 19 and 20, together with consequential changes to the appointment framework of the DPDP Act, 2023. Although section 19 already prescribes broad eligibility criteria, the framework should contain more objective and specialized qualifications and stronger appointment safeguards, fixed or sufficiently secure terms of office, appropriate safeguards governing tenure and removal, and institutional protections consistent with constitutional principles applicable to adjudicatory and regulatory bodies. Additional appointment safeguards may modestly increase the complexity of establishing and maintaining the Board. That concern is outweighed by the need to ensure that a body responsible for adjudicating data-protection contraventions, including those involving public authorities, enjoys sufficient institutional independence from the executive.

3.5.5 A Narrower and Reviewable Exemption Power for Mental Health Data

Further, Section 17(2) of the DPDP Act, 2023 should be amended so that, at least with respect to the mental health information processing, exemption notifications identify the specific statutory provisions being displaced, operate only for a defined period, remain subject to periodic parliamentary review, and are accompanied by an appropriate mechanism of independent oversight. The rationale underlying section 17(2) should not be discounted. The rationale behind section 17(2) should not be dismissed. Sovereignty, public order and national security are legitimate concerns, and there will be occasions where they justify departing

from the ordinary consent-based principles. The constitutional question, then, is not whether such exemptions should exist at all, but whether their scope and manner of operation are properly defined, necessary, proportionate and open to review. An exemption power that is tightly defined, time-bound and subject to independent review would offer far stronger safeguards for psychiatric information than one built without these procedural constraints.

3.5.6 A Risk-Based, Not Volume-Based, Significant Data Fiduciary Threshold for Mental Health Data

Section 10 already recognises that the volume and sensitivity of personal data, along with the risk posed to data principals, are relevant factors in designating a Significant Data Fiduciary. The gap lies not in any exclusion of sensitivity from this framework, but in the absence of a rule that automatically imposes heightened obligations on entities processing highly sensitive categories such as psychiatric information. A small entity handling mental health records may in fact pose a greater privacy risk than a much larger entity processing ordinary personal data. The designation framework should therefore account for the inherent sensitivity of psychiatric data and its potential consequences, even where the volume processed is low. This approach would better reflect the constitutional weight given to protecting psychiatric information and would tie regulatory obligations to actual risk rather than to volume-based criteria that may fail to capture small-scale but high-sensitivity processing.

3.5.7 Institutional Coordination

Finally, formal mechanisms for coordination should be built into the DPDP Act, 2023 and the MHA, 2017, linking the Data Protection Board with the concerned State Mental Health Authorities and the Mental Health Review Boards. Guidance issued under the Ayushman Bharat Digital Mission should be brought in line with this coordinated structure, so that the collection, processing, disclosure and retention of mental health information are governed by consistent standards across India's digital healthcare ecosystem. Stronger coordination among these institutions would cut down regulatory fragmentation, reduce overlapping compliance requirements and move the governance of mental health information toward a more coherent system overall.

4. Conclusion

The analysis undertaken demonstrates that the principal challenge in protecting mental health information in India does not arise from any fundamental deficiency in either the MHA, 2017 or the DPDP Act, 2023 when each is considered independently. The MHA, 2017 represented a significant shift in Indian mental health law by placing mental health confidentiality on an express statutory footing as a right of persons with mental illness. The DPDP Act, 2023, in turn, establishes a general statutory framework for digital personal-data protection against the constitutional backdrop created by *Justice K.S. Puttaswamy (Retd) v Union of India*. The principal shortcomings identified emerge from the interaction between these two statutory regimes rather than from either statute in isolation. Those shortcomings include the absence of an automatic category of enhanced protection for sensitive personal data, as well as the psychiatric information, the absence of any meaningful coordination between the DPDP Act's consent framework and the capacity-based model established under the MHA, 2017, the breadth of the exemption power contained in section 17(2), and an institutional framework that does not adequately integrate mental health regulation with data protection oversight.

These shortcomings can be corrected through legislative and institutional change. The notification of the DPDP Rules, 2025 and the establishment of the Data Protection Board show that India's data protection framework is still developing, not that it has reached a final, settled form. The reforms set out in Part 3.5 are meant to build on this evolving framework rather than displace it, with the shared aim of ensuring that the governance of mental health information accounts for the distinctive risks psychiatric data carries, while staying true to the constitutional values of dignity, autonomy and informational privacy.

At bottom, mental health information cannot be adequately protected by two statutory regimes running in parallel without any real coordination between them. A psychiatric record is not merely one more category of health data. Its disclosure carries legal, social and personal consequences of a different order, consequences that call for a more integrated approach to governance than Indian law currently offers. Meeting that objective will require mental health law and data protection law to work more closely together, functioning as complementary safeguards for the same individual rather than as separate systems pursuing parallel goals.

5. Acknowledgments

The authors thank the School of Law, Sushant University, Gurugram, for the support in preparing this article.

Conflict of Interest: The author declares no conflict of interest, financial or otherwise, in relation to this article.

Funding: No funding was obtained for this article.

6. References

1. Ranade K, Kapoor R, Fernandes S. Mental Health Law, Policy and Program in India: a fragmented narrative of change, contradictions and possibilities. SSM Ment Health. 2022;2:100174. DOI: 10.1016/j.ssmmh.2022.100174
2. Mental Healthcare Act, 2017 (India).

3. Goyal N, Agrawal T. Operationalizing ethical, privacy, and data security frameworks in India's digital health ecosystem. Int J Ayurveda Res. 2026;7(1):72. DOI: 10.4103/ijar.ijar_278_25
4. Duffy RM, Kelly BD. Privacy, confidentiality and carers: India's harmonization of national guidelines and international mental health law. Ethics Med Public Health. 2017;3(1). DOI: 10.1016/j.jemep.2017.02.018
5. Adhithya GM, Keerthana K. Data privacy and protection in India: a critical doctrinal analysis of the Digital Personal Data Protection Act, 2023 in the light of constitutional standards and international benchmarks. Indian J Legal Rev. 2026;6(7):13. DOI: 10.65393/IJLRV6I73
6. Mr X v Hospital Z (1998) 8 SCC 296 (India).
7. Hindu Marriage Act, 1955 (India).
8. Biswas S. Experts talk about the patient's right to confidentiality while seeking therapy. Times of India. 2020. https://timesofindia.indiatimes.com/life-style/health-fitness/de-stress/experts-talk-about-the-patients-right-to-confidentiality-while-seeking-therapy/articleshow/78187748.cms
9. MP Sharma v Satish Chandra AIR 1954 SC 300 (India).
10. Kharak Singh v State of UP AIR 1963 SC 1295 (India).
11. Gobind v State of Madhya Pradesh (1975) 2 SCC 148 (India).
12. People's Union for Civil Liberties v Union of India (1997) 1 SCC 301 (India).
13. Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (India).
14. Justice K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (India).
15. Digital Personal Data Protection Act, 2023 (India), No. 22 of 2023.
16. Information Technology Act, 2000 (India).
17. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
18. Jain D. Regulation of digital healthcare in India: ethical and legal challenges. Healthcare (Basel). 2023;11(6):911. DOI: 10.3390/healthcare11060911
19. Sethi MIS, et al. The Digital Personal Data Protection Act 2023: implications for mental healthcare practice in India. Indian J Psychol Med. 2025. DOI: 10.1177/02537176251370651
20. Digital Personal Data Protection Rules, 2025 (India).
21. Rights of Persons with Disabilities Act, 2016 (India).
22. Ministry of Electronics and Information Technology. Digital Personal Data Protection Rules, 2025. Gazette of India, Extraordinary, Part II, Section 3(i). 2025 Nov 13.
23. Press Information Bureau. DPDP Rules, 2025 notified. Government of India; 2025 Nov 14.
24. United Nations Convention on the Rights of Persons with Disabilities. 2515 UNTS 3. Adopted 2006 Dec 13; entered into force 2008 May 3.
25. R Gandhi v Union of India (2010) 11 SCC 1 (India).