Pathology of Consent in India's Digital Health Ecosystem: Privacy, Proportionality, and Right to Health

Mohd Rameez Raza*

ABSTRACT

India has been actively promoting digital healthcare infrastructure under DPI, and the enactment of the Digital Personal Data Protection Act has given rise to new jurisprudence. The Act introduced a granular and transactional model of consent in the digital healthcare domain. Though it attempts to protect privacy in line with Puttaswamy 2017, the broader argument is that the Act's highly granular and restrictive consent requirements result in substantial procedural complications. Such complications translate into barriers in practice, creating consent fatigue, function creep, and access disparities. This paper critically examines the contradictions between healthcare and privacy in the context of the 'pathology of consent' developed by Richards and Hartzog. The current conceptualisation of consent in India is a benign theory that serves as a protective instrument, but is a prohibitive wall in reality. Such a proposition is constitutionally unacceptable as it defeats access to equitable healthcare in the constitutional ambit. Further, the paper attempts to establish that consent should not be approached in a binary manner, but proportionately and within a context. In conclusion, advocating for the use of dynamic, broad, or presumed consent models to develop a protective and inclusive ethos that positions India on the map of public health and data commons.

Keywords: Consent, DPDP, ABDM, Puttaswamy, Data Commons, Granular Consent.

***

* **Mohd Rameez Raza** is a Teaching Assistant and LL.M. in Technology and Law Candidate at Hidayatullah National Law University, Raipur. *Acknowledgements*: The author expresses sincere gratitude to **Prof. (Dr.) Yogendra Kumar Srivastava**, Professor of Law at Hidayatullah National Law University, for his invaluable guidance from the ideation stage of this paper, as well as for his constructive feedback and review. The author also thanks **Yugal Bhatt** for peer-review during the final stage.

1. INTRODUCTION

India is actively seeking to achieve universal health coverage with improved administrative efficiency. Ayushman Bharat Digital Mission ("ABDM" *hereinafter*) was implemented to achieve the goal by creating an interoperable ecosystem of patients, medical practitioners, personnel, and healthcare institutions. ABDM is focused on collecting, processing, and storing data with a unique Ayushman Bharat Health Account ("ABHA" *hereinafter*) as a vault. The final stage of ABDM is developing comprehensive health registries with longitudinal records for interoperability and analytics.[1]

The Digital Data Protection Act ("DPDP Act" *hereinafter*) regulates every facet of the data, from the collection of data, to processing it, and lastly storage of data,[2] ensuring the privacy established in Puttaswamy 2017,[3] in the ABDM framework. The Act also ensures control of health records and data is in accordance with the consent framework, and shall be comprehensively established within informed consent, data minimisation, and accountability ambit.[4]

India's data protection regime highlights its unique balance between individual consent and substantive fairness. Data fiduciaries are responsible for fair and reasonable processing, arguing this goes beyond the often-flawed consent models prevalent elsewhere.[5] The consent framework under the DPDP requires granular, transaction-specific approvals as a mandatory requirement.

However, a critical friction is emerging at the confluence of these well-intentioned privacy safeguards and the practical realities of healthcare access. Striking a balance between public good and privacy is a challenge under the current DPDP Act.[6] Such a stringent, transaction-specific interpretation of consent is theoretically empowering, but it creates significant procedural hurdles that can obstruct, delay, and even deny timely healthcare, disproportionately

[1] National Health Authority, *A brief guide on Ayushman Bharat Digital Mission (ABDM) and its various building blocks* (White Paper, Version 1.1, 2021) ch 5
[2] Digital Personal Data Protection Act 2023, s 4 & 6
[3] *Justice K.S. Puttaswamy (Retd.) v Union of India,* (2017) 10 SCC 1
[4] Vasudha Khanna & Atul Kotwal, 'Examining the Significance of the Digital Personal Data Protection Act 2023 in the Context of the Healthcare Industry: A Comprehensive Analysis' (2025) 22 Discover Public Health 381, 1
[5] Mark J. Taylor & Jeannie Marie Paterson, 'Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection' (2020) 16 Indian Journal of Law and Technology 1, 71
[6] *Id*

affecting socio-economically marginalised individuals.[7] thereby undermining healthcare, which is ensured under Article 21.

Richards and Hartzog critique such an over-reliance and step-by-step or transactional model of consent in digital environments by introducing a vocabulary of 'consent pathologies.' They argue that meaningful consent is only possible under specific conditions: infrequent requests, vivid risks, and significant stakes, which are rarely present online.[8]

Fairness standard, if robustly applied, can provide stronger protections against the shortcomings of consent, questioning whether data protection should serve only individual autonomy or also enforce broader rights, like the right to health.[9] Digital healthcare as a data infrastructure creates new power dynamics and changes how access to healthcare is mediated by data-driven systems. Current digital health regime balances privacy and public good, but the socio-legal impact of consent requirements and implementation of ABDM creates procedural friction in accessing digital health services, especially for vulnerable populations and may infringe upon their right to timely and equitable healthcare.

This paper investigates the legal frameworks, constitutional principles, and socio-legal implications of the consent regime within India's digital healthcare ecosystem and ABDM's data protection in the ambit of the DPDP Act, which is affecting access to healthcare. Especially for the vulnerable and marginalised groups, barriers that violate the right to health, causing an imbalance between public good and data protection.

Further, this paper also critically analyses this friction and examines the barrier to accessing digital health services within the ambit of consent, privacy, and health. In conclusion, highlight the need to adopt a broad and contextual model of consent to ensure constitutional balance, while keeping the spirit of Puttaswamy 2017 alive, and suggest revisiting the consent model in a more context-sensitive and pragmatic framework that balances data protection and equitable delivery of healthcare services in India.

[7] Ramya Chandrasekhar, 'Datafication, Power, and Publics in India's National Digital Health Ecosystem' (2024) 20 Socio-Legal Review 1, 1
[8] Neil Richards & Woodrow Hartzog, 'The Pathologies of Digital Consent' (2019) 96 Washington University Law Review 6, 1461
[9] Note 5

2. CONSTITUTIONAL AND LEGAL TAKE ON PRIVACY AND HEALTH

ABDM's effectiveness is predicated on the assumption that every patient is digitally literate, has consistent access to a smartphone and internet, and can make informed decisions in real-time, often under the duress of illness.[10] This assumption is deeply flawed in a country as diverse and digitally stratified as India.

2.1. Consent after Puttaswamy 2017

Puttaswamy 2017 recognised that privacy includes informational privacy, which encompasses an individual's right to control their data. Though privacy is not an absolute,[11] it must satisfy the three-pronged test of legality, necessity, and proportionality for restriction. Proportionality is most relevant here as it mandates that infringement must be proportionate and only until the objective sought to be achieved.[12] A measure that imposes excessive or disproportionate burdens on the right-holder would be unconstitutional.[13]

The proportionality test is the standard to which the operation of the consent structure in the ABDM must be held. If obtaining consent is made so complex as to, in effect, deny access to a fundamental right like health care, it may fail the proportionality test. Puttaswamy 2017 thus provides the constitutional base for consent as a key element of informational self-determination.[14]

2.2. DPDP evolved the idea of Consent

Section 6 states that consent must be sought through notice, be purpose-specific, and must be free, informed, unconditional, and that can be revoked at any time.[15] This implies that a blanket or bundled consent for multiple purposes is invalid. ABDM should also require a distinct processing activity, a fresh consent, as may be required.

[10] Deekshitha Ganesan 'Human Rights Implications of the Digital Revolution in Health Care in India' (2022) 24 Health and Human Rights Journal 1, 5
[11] Digital Personal Data Protection Act 2023, s 6
[12] Shruti Trikanad, 'Disproportional Proportionality: An Analysis of the Proportionality Test, Aadhaar, and Digital ID' (*Indian Journal of Law and Technology*, 1 July 2022) <https://www.ijlt.in/post/disproportional-proportionality-an-analysis-of-the-proportionality-test-aadhaar-and-digital-id> accessed on 29 January 2026
[13] Severyna Magill, 'The Right to Privacy and Access to Abortion in Post-Puttaswamy World' (2020) 2020 University of Oxford Human Rights Hub Journal 2, 160
[14] Note 3
[15] Note 2

While the Act also introduces the concept of 'deemed consent' in certain situations, e.g., for the performance of state functions, compliance with law, or in medical emergencies,[16] the primary ground for processing remains explicit consent.

In a health care context, what we see is a patient giving consent for a health care visit, then a separate one for a diagnostic test, and also separate consent to share that report with another specialist. While at first it may seem to put power in the hands of the patient, this granular approach is where we see the issues play out. The Act's strict interpretation in turn puts forth a very narrow view of consent, does not in fact protect as much as it does act as a bureaucratic road block, which in turn disrupts the continuity of care.[17]

2.3. Health vis-à-vis Constitution

India, through a series of progressive interpretations, has recognised health and access to it as an integral component of the constitutional framework. In cases like Paschim Banga Samity, established that "the failure of a government hospital to provide timely medical treatment to a person in need of emergency care results in a violation of their right to life".[18] Further, in Common Cause same was reiterated that "the State has a positive obligation to provide healthcare access and ensure that its systems do not create unreasonable restrictions".[19]

The argument pushes onto the state a passive constitutional concern. An environment that is conducive to good health must be created, in addition to avoiding actions that can harm a person's health. It is also important to ensure that the health care system does not contain unnecessary systemic or administrative barriers to care. A digital health platform, which seems to have the credible objective of efficiency, puts up consent-related challenges that lead to the exclusion of that access; it breaches the scope of the State's obligation as articulated in Article 21. Access to healthcare is not the only component of the right to health; it is the access to healthcare when and how it is needed, time is the essence in this.[20]

[16] Digital Personal Data Protection Act 2023, s 7
[17] Vasantha Kotagiri and Poorvi Baliga, 'Strengthening Digital Infrastructure in The Health Sector: An Assessment of Recognition to Digital Privacy' (2023) 5 CMR University Journal for Contemporary Legal Affairs 3, 174
[18] *Paschim Banga Khet Mazdoor Samity v State of West Bengal*, (1996) 4 SCC 37
[19] *Common Cause v Union of India*, (2018) 5 SCC 1
[20] Note 10

3. CONSENT DESIGN OF ABDM

The ABDM operationalises the principle of consent through a technology-enabled architecture consent manager called Health Information Exchange Consent Manager ("HIE-CM" *hereinafter*). The ABDM framework is designed to ensure that no health data is shared without the patient's explicit approval. The process typically involves a healthcare institution's request for health records, which is routed to HIE-CM via a unique ABHA ID, and the data subject receives a notification detailing the request, purpose, and data sought. The data subject may accept or deny the request, along with the duration for which the data may be accessed.

The theoretical elegance of the ABDM's consent framework belies its significant practical challenges. These challenges are not merely technical glitches but systemic issues that create a gap between the law's intent and its real-world impact, particularly for the most vulnerable and marginalised groups in society.

3.1. Operational Challenges in Obtaining Consent

The need for specific transactional consent is the major point of friction. During their journey through the healthcare system, a patient encounters various steps and many different people. Let's take an example: A patient receiving an outpatient consultation is referred to a specialist after laboratory tests and a radiology scan. Both medical professionals should now have access to the report for diagnosis. In the current ABDM consent framework, patients must consent separately to both the medical professional (outpatient consultant and specialist) via a mobile app, which may lead to consent frustration or exclusion due to the mobile app's unavailability.

ABDM's transactional, granular consent model is less effective and more challenging for larger populations. Most severely impacted in this divide will be daily wage workers with limited access to smartphones, the elderly who depend on caregivers, who may also find the granular consent complicated, leading to exclusion,[21] and illiterate people.[22]

For populations mentioned above, consent mechanisms have evolved from empowering instruments into methodical obstacles. This directly oversteps their right to health under Article 21, creating a new form of digital exclusion in the most critical of sectors. The obligation of

[21] Anumeha Yadav, 'Companies Gain, Elders Lose in Rajasthan's Turn to "Cradle to Grave" Digital Governance' (*The Wire*, 25 August 2025) <https://thewire.in/rights/companies-gain-elders-lose-in-rajasthans-turn-to-cradle-to-grave-digital-governance> accessed on 12 February 2026
[22] Note 10

the state, stated in Common Cause, to provide healthcare without unreasonable restrictions is seemingly violated by a state-mandated system that disproportionately burdens the vulnerable.[23]

3.2. Judicial Precedents questioning ABDM

While Puttaswamy 2017 established the primacy of privacy, the judiciary has consistently sought to balance competing rights. Although the principle of proportionality is key, as a measure, it is disproportionate and has a negative impact on a fundamental right, outweighing the benefits it seeks to achieve.[24] In ABDM, the rigid application of granular consent may be disproportionate in healthcare delivery. While protecting privacy is a legitimate state aim, doing so in a manner that creates life-threatening delays or excludes entire populations from care cannot be considered a proportional measure.[25]

On the other hand, judgment in Common Cause reinforces the state's positive obligation to facilitate healthcare.[26] The Court's recognition of the right to die with dignity, including passive euthanasia[27], was also rooted in the patient's autonomy over their own body, which animates the concept of consent.[28] However, the judiciary has always balanced individual autonomy with the state's interest in preserving life and public health. However, the consent framework in ABDM is so rigid that it prevents doctors from accessing critical information promptly, which undermines this broader public health interest.

The issue is out in the open; the DPDP Act and the ABDM framework set out a protective stance, prohibition as the default rule until consent is given. On the other hand, we see that the success of health care delivery depends on the smooth and rapid flow of information. In an emergency, the need for digital consent before access to a patient's medical history, past care, and laboratory reports may mean the difference between life and death. Although the Act has made an exception for medical emergencies, it is unclear what it defines, and its application

[23] Note 19
[24] Z. Zakhar Naved and Isha Kaushal, 'Aadhaar: Its Implementation and Implications' (2019) 8 Christ University Law Journal 1, 1
[25] Note 8
[26] Note 19
[27] *Aruna Ramchandra Shanbaug v Union of India*, (2011) 4 SCC 454
[28] Sushila Rao, 'India and Euthanasia: The Poignant Case of Aruna Shanbaug' (2011) 19 Medical Law Review 4, 646

within the ABDM framework is a difficult process, which again is a fine line between life and death.

The conflict is not with the principle of consent itself, but with its current inflexible and technology-centric implementation. The system is designed with data protection as the primary consideration and healthcare delivery as the secondary consideration. This needs to be inverted. The primary goal of a health information system should be to improve health outcomes; data protection is a critical, coequal objective, but it should not supersede the primary purpose of saving lives and promoting well-being.

4. Comparative Jurisprudence and Best Practices

GDPR has served as a model for data protection frameworks. Like the DPDP Act, it places great value on explicit consent and has adopted a broad-brush approach to processing sensitive data, including health data in particular. Article 9(2) reports that health data may be processed for preventive or occupational health, diagnostic, and social care purposes without obtaining explicit consent.[29] Health records in the health registry are used for research and analysis, which in the end will support public health through predictions in pandemic-like situations. The GDPR framework also notes that the use of health data solely on the basis of consent is impractical in healthcare settings.

Unlike the GDPR's consent-first model, HIPAA operates on a system of permitted uses and disclosures; it allows 'covered entities', i.e., healthcare providers and insurers, to use and disclose data without obtaining patient authorisation for each specific use.[30]

For example, a hospital can share a patient's records with a specialist at another hospital for consultation purposes without seeking fresh consent, as this falls under 'treatment.' While patients are given a notice of privacy practices and have the right to request restrictions, the default is that information flows freely for core healthcare functions.[31] The HIPAA model prioritises the continuity of care, reducing the consent burden for routine clinical activities.[32]

[29] General Data Protection Regulation 2018, art. 9(2)
[30] Health Insurance Portability and Accountability Act 1996
[31] HIPAA Privacy Rule 1996, s 160.103
[32] Deven McGraw & Kenneth D. Mandl, 'Privacy protections to encourage use of health-relevant digital data in a learning health system'(2021) 4 NPJ Digital Medicine 1, 2

5. Reforms needed in ABDM Consent Framework

Reforming India's consent framework does not mean abandoning data protection; it means designing a smarter, more humane system that is constitutionally sound, statutorily compliant, and practically feasible. This requires moving towards a context-sensitive consent model.[33]

5.1. Context-Sensitive Consent Model

The blanket approach to consent is not suited to India's diverse healthcare infrastructure. The law must differentiate between different contexts of data sharing.[34] Sharing data with a primary care physician for treatment is fundamentally different from sharing it with a pharmaceutical research company. In a context-sensitive model, it is justified by the constitutional principle of proportionality; the burden of consent should be proportional to the risk and purpose of the data processing[35]. The following models could be adopted:

Broad Consent: At the primary treatment stage within a healthcare facility or a network of trusted providers, patients could be given the option to provide 'broad consent.' This would authorise doctors and labs directly involved in their care to access their health records for the duration of that specific treatment episode without requiring repeated digital approvals. This consent would still be informed and specific to the purpose of treatment, but would apply to the entire episode of care, reducing friction.

Dynamic Consent: In the secondary stage, uses of data, such as for research or public health analysis, a more interactive 'dynamic consent' model should be implemented. This would allow patients, through a simplified interface, to set their preferences for how their anonymised or pseudonymized data can be used. They could opt in or opt out of specific types of research, giving them meaningful control without hindering valuable medical research that serves the public good.

Presumed Consent: In officially declared epidemics or public health emergencies, a model of presumed consent (or an opt-out model) for the sharing of anonymised public health data with government agencies should be legally enabled. This is crucial for rapid response, contact tracing, and resource allocation. GDPR's public interest exceptions provide a strong precedent

[33] Note 8
[34] Anthony H. Szczygiel, 'Beyond Informed Consent' (1994) 21 Ohio Northern University Law Review 21, 171
[35] Ella Corren, E, 'The Consent Burden in Consumer and Digital Markets' (2022) 36 Harvard Journal of Law & Technology 36, 551

for this. Such a measure would be a necessary and proportionate restriction on privacy to serve the legitimate state aim of protecting public health, fully compliant with the Puttaswamy 2017 test.

5.2. Affirmative Approach for Consent

Primarily, the DPDP Act, which is its tool for rule-making, shall put in place particular provisions for health data, and the term 'healthcare data' put forth as a separate category, which is what we have in the GDPR. Secondly, the HIE-CM structure should be reworked to support many consent models. We should see in it options for 'broad consent' for the duration of a health issue, and also 'dynamic consent' for secondary uses.

Thirdly, the large-scale implementation of accessible design in how consents are obtained from users via mobile apps and other platforms. This includes the use of multiple languages, simple icons and also options for caregivers to give legal consent on a dependent's behalf. Finally, must put in place and integrate into our systems a very strong and legal way to give consent, which may include physical consent forms or IVR systems, which in turn connect to the patient's ABHA ID.

The adoption of context-based consent frameworks would mean developing large-scale public initiatives to help people understand their data rights related to the ABDM and DPDP Act, the types of consent, and how to exercise their preference management. It would also mean that healthcare providers must complete extensive training about the data fiduciary responsibilities and the informed consent mechanisms that maintain the privacy and timeliness of treatment. The first iteration of the proposed consent frameworks should be implemented in various geographic and socio-economic areas to understand the problems and make adjustments before a country-wide adoption.

6. Conclusion

The transition from a traditional health care system to a digital health care system in India is a very important step. ABDM is such a step towards health care delivery, and the DPDP Act puts in place the protection for the health data and privacy required for ABDM. At the same time, we see issues with the present digital health delivery model, which may nullify the results.

What we have at present is a very detailed and specific structure, which may, in fact, do the opposite of what it is intended to do by creating large-scale operational problems. What should have been a positive change ends up in practice doing the opposite; it is, in fact, defeating health as a right and health equity. ABDM is not designed for the less privileged and the illiterate population, which, in turn, is to a significant degree adding to the inequality we are trying to eliminate.

The contestation around the contemporary idea of consent, the much narrower approach to the data protection principles, and the absence, or the likely absence, of the constitutional test of proportionality in the foundational constitutional right to health care, is fundamental. The attempt is not to breach the privacy of the individual, but rather to identify a point of equilibrium. 'Equilibrium' in this instance entails that the right to privacy, the right to free circulation of information, and the right to non-discriminatory, equal, and accessible healthcare are all structural provisions of the constitutional order.

India should take inspiration from the global allies and must pick up the best practices[36] from their consent framework and data protection regime.[37] Unlike other countries, India's healthcare institutions and practitioners should serve citizens from various strata and, therefore, require a flexible and context-sensitive consent framework. Adopting a blanket model would lead to a large section of the population being excluded from the healthcare fold. Research and analytics, supported by data, must also be balanced. More needs to be done concerning consent and data protection, the associated technology, and the framework of inclusiveness and diversity. ABDM will succeed only if its best possible frameworks are designed to serve the largest number of citizens.

***

[36] Veronika Almasi, 'Overview of the Digital Healthcare in Hungary' (2024) 2024 Studia Universitatis Babes-Bolyai Jurisprudentia 2, 128

[37] Yasaman Abbaszada, 'Digital Transformation in Healthcare Systems: Challenges and Opportunities' (2025) 19 AGORA International Journal of Juridical Sciences 1, 147