INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 3 | 2026 Art. 24

Patient Rights, Informed Consent and Health Data Protection in the Digital Age: A Critical Analysis of India's DPDP Regime and Emerging Digital Healthcare Practices

Tauseef Parvez
Research Scholar
Faculty of Law
Aligarh Muslim University, Aligarh

Rizwan Ahmad
Research Scholar
MANUU Law School
Maulana Azad National Urdu University, Hyderabad

Recommended Citation
Tauseef Parvez and Rizwan Ahmad, *Patient Rights, Informed Consent and Health Data Protection in the Digital Age: A Critical Analysis of India's DPDP Regime and Emerging Digital Healthcare Practices*, 5 IJHRLR 366-377 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Patient Rights, Informed Consent and Health Data Protection in the Digital Age: A Critical Analysis of India's DPDP Regime and Emerging Digital Healthcare Practices

ABSTRACT

The rapid digitisation of the healthcare sector via telemedicine, AI-based diagnostic technologies, and electronic health records has changed the doctor-patient relationship in India, and the situation has become complicated due to issues of patient rights, informed consent, and health data security. Although both the Digital Personal Data Protection Act, 2023. and the draft DPDP Rules, 2025 provide a rights-based, consent-centric approach, there are still major grey areas in regard to the sensitive health data. The main research issue that is identified in this paper is the normative and operational disconnection between the traditional medical consent and data protection consent in digitally mediated healthcare ecosystems. The paper has three focus areas: (i) Discuss the extent and enforceability of patient rights under the DPDP regime; (ii) Discuss the changing doctrine of informed consent when it comes to continuous and secondary healthcare practices that are facilitated by AI (iii) Discuss how sufficient the legal framework in India is to combat the risks posed by AI-enabled and platform-based healthcare practices. The study embraces a doctrinal and comparative approach to the study, which refers to statutory analysis, policy reports and the ongoing review of DPDP provisions by the Supreme Court (2026). This paper, argued that the DPDP framework enhances informational autonomy by imposing the consent conditions, it is still inadequately prepared to cope with the sector-specific issues, including the utilization of secondary data, the regulation of clinical research, and the decision-making of algorithms. It concludes that the Indian data protection framework is an indication of a transition to the digital dignity and patient-centric governance, but it needs regulatory harmonisation and enforcement to be strengthened to provide effective protection of patient rights.

KEYWORDS

Patient Rights, Informed Consent, DPDP Act 2023, Health Data Protection, Digital Healthcare

1. INTRODUCTION

Healthcare in India is now quickly being digitalised with telemedicine, AI-based diagnostics, electronic health records (EHRs) and the Ayushman Bharat Digital Mission (ABDM), which is converting care into a platform-based, data-driven system.[1] By 2025, the digital health market is estimated to hit USD 10-15 billion,[2] whereas the consumption of telemedicine has grown more than three times in the post-COVID-19 period, which is an indication of a sharp transition towards virtual models of healthcare.[3] Health data has become a valuable economic resource in this dynamic ecosystem, commonly described as the new oil, and its collection, processing, and commercialization has become a contentious issue.[4]

The normative power of patient rights in India is based on constitutional issues. The Supreme Court acknowledged the right to privacy in *Justice K.S. Puttaswamy v. Union of India (2017)*[5] as it acknowledged the right to informational privacy and control of personal information, which were not explicitly mentioned in Article 21. This has a direct implication on digital healthcare where sensitive health information is regularly processed by both government and private organizations. Equally, the principles of dignity, bodily autonomy and informed consent have been enforced in *Common Cause v. Union of India (2018)*[6] *and X v. Principal Secretary, Health and Family Welfare Dept., Govt. of NCT Delhi*,[7] the Court supported the idea of patient choice as the key aspect of medical decision making. All these decisions create a constitutional nexus between privacy, consent, and patient rights in the digital era.

The Digital Personal Data Protection Act, 2023 is the major legislative initiative towards data protection in India.[8] But with its sector-neutral design, there is a question mark as to whether it is sufficient to deal with the increased sensitivity of health data.[9] The paper is doctrinal and will analyse the judicial precedents, statutory framework and policy reports,

[1] Ministry of Health & Family Welfare, *Ayushman Bharat Digital Mission: Strategy Overview* (Gov't of India 2022).
[2] NITI Aayog, *Digital Health in India: Emerging Opportunities* 12–14 (2020).
[3] McKinsey & Company, *Telemedicine: A Quarter-Trillion-Dollar Post-COVID-19 Reality?* (2021).
[4] Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 6–10 (Houghton Mifflin Harcourt 2013).
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.
[6] *Common Cause v. Union of India*, (2018) 5 S.C.C. 1
[7] *X v. Principal Sec'y, Health & Fam. Welfare Dep't, Gov't of NCT of Delhi*, (2022) 10 SCC 1.
[8] Digital Personal Data Protection Act, No. 22 of 2023, https://www.indiacode.nic.in/. (last visited Apr. 10, 2026).
[9] Graham Greenleaf, *India's New Data Protection Act: The Good, the Bad and the Unclear*, 169 Privacy L. & Bus. Int'l Rep. 1, 3–5 (2023).

qualitative data on the user behaviour, and quantitative data on the market growth, and the adoption trends. It asserts that despite the DPDP Act being a significant step towards data governance, it has structural constraints to support the autonomy of patients, meaningful informed consent, and health data integrity in a more digitised healthcare ecosystem.

2. PATIENT RIGHTS AND INFORMED CONSENT IN THE DIGITAL AGE

2.1 Legal Framework of Patient Rights

Law dictates the rights of patients and this paper will discuss the legal environment of patient rights. The Indian law of patient rights is rooted in the following concepts privacy, confidentiality and autonomy of which ensure the fact a person has the right to manage his/her personal and medical data.[10] These rights have been developed with the help of the judicial precedents. The case of *Samira Kohli v. Dr. Prabha Manchanda (2008)* emphasized that the consent must be real, informed and specific and had not recognised the validity of the vague or blanket authorisation given in the medical procedures.[11] Other case *Mr. X v. Hospital Z (1998)* addressed the case of confidentiality and the Court determined that the unauthorised release of medical condition of a patient may result in considerable reputational and personal harm, therefore the necessity to protect sensitive health information.[12] The fact that the rights of patients are not procedural is established by them, and is directly linked to dignity and autonomy.

2.2 Transformation of Consent in Digital Ecosystems

The process of digital healthcare ecosystems migration has completely transformed the character of the informed consent. Consent in the digital environment in contrast to traditional face-to-face medical communication is normally signed as a click-wrap agreement and as an application-based consent.[13] These processes increase efficiency and scalability at the expense of knowing, and it is concerning that these instruments of informed choice are thought to be as legitimate. Research shows that a considerable number of users have not read or completely understood the privacy policies before consenting, and this fact negates the usefulness of consent data protection systems.[14] Consent thus turns into a formality instead of a substantive exercise of patient autonomy and

[10] *Puttaswamy*, supra note 5.
[11] *Samira Kohli v. Dr. Prabha Manchanda*, (2008) 2 S.C.C. 1
[12] *Mr. X v. Hospital Z*, (1998) 8 SCC 296 (India Supreme Court).
[13] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[14] Id.

negates the very tenets as expressed in the judicial precedents.

3. INDIA'S DPDP ACT, 2023 AND HEALTH DATA GOVERNANCE

3.1 Core Structure of the DPDP Regime

The Digital Personal Data Protection Act, 2023 (DPDP Act)[15] creates a consent-based system of the processing of personal data in India based on the relations between the Data Principal and the Data Fiduciary. The Act requires that processing of personal data can only be done with valid consent with some exception of justifiable uses hence giving a lot of weight to individual control of personal information. It also gives a series of enforceable rights to the data principals which include the rights to access information, demand correction and request erasure of personal data. Although these provisions are an example of a rights-based approach that would be consistent with the global data protection requirements, their efficacy in the situation with sensitive health data would be greatly determined by the way they are implemented into practice and adapted to the specifics of their sector.[16]

3.2 Application to the Healthcare Sector

The DPDP Act is highly applicable to all entities that process personal data, which includes hospitals, insurers and an ecosystem of health-technology platforms that is rapidly growing.[17] This encompasses telemedicine, digital health apps and wearable devices that periodically gather and analyze sensitive health-related data. It is reported that there is a growing usage of private health applications with the national digital health infrastructure, especially in the Ayushman Bharat Digital Mission (ABDM), which results in an increase in the level of interoperability and data exchange across platforms.[18] Although this integration is effective and more convenient, it also increases the issue of data exchange, consent, and abuse of sensitive medical data between systems which are connected with each other.[19]

3.3 Informed Consent in Digital Healthcare: Policy vs. Reality

Although formal protection is offered on the basis of the DPDP framework, empirical data show that there are important issues related

[15] DPDP Act, supra note 8.
[16] Graham Greenleaf, India's New Data Protection Act: The Good, the Bad and the Unclear, 169 *Privacy Laws & Bus. Int'l Rep.* 1 (2023).
[17] Id.
[18] Ministry of Health & Family Welfare, *Ayushman Bharat Digital Mission: Operational Framework* (2022).
[19] Id.

to the effective operation of the digital health data governance.[20] Research indicates that more than 60 percent of health-technology platforms are based on the third-party data-sharing schemes, usually with collaboration with analytics companies, insurers, and other business organizations. This pose doubts on how aware and specific user consent is. Also, the healthcare sector is reported to have been ranked as one of the most targeted industries as the amount of healthcare related data breaches is steadily increasing all over the globe owing to the fact that medical information is highly valued.[21] These numerical measures illustrate an irrelevance between normative data protection framework and the functionalities of the digital healthcare ecosystem where economic incentives tend to encourage broadly data usage.

4. EMERGING DIGITAL HEALTHCARE PRACTICES AND RISK LANDSCAPE

4.1 Digital Health Infrastructure and technologies

Digital health ecosystem in India is increasingly playing an important role with integrated platforms and technology-based solutions. Ayushman Bharat Digital Mission will focus on creating a single health data infrastructure, through interoperability across hospitals, laboratories, and digital health apps. In line with this framework, the Telemedicine Practice Guidelines, 2020 have validated remote consultations, which have greatly relieved access to healthcare services.[22] Electronic Health Records systems also promote continuity of care by ensuring that information about patients is systematically stored, and shared.[23]

At the same time, new technology, such as AI-based diagnostics and wearable health-related gadgets, made healthcare delivery an information-intensive process that is perpetually ongoing. Although these innovations enhance efficiency and accessibility, they also make data collection bigger and more sensitive.

4.2 Ground-Level Challenges

There are a number of systemic issues, which impede the successful safeguarding of health data at the implementation level. A lack of awareness of patients about their rights to data and online privacy greatly hampers the capability of people to have control over their information. This is aggravated by the fact that most healthcare facilities

[20] Solove, supra note 13.
[21] IBM Security, *Cost of a Data Breach Report 2023* (2023).
[22] Telemedicine Practice Guidelines, 2020, Ministry of Health & Family Welfare, India.
[23] World Health Organization., *Global Strategy on Digital Health 2020–2025* (2021).

have weak cybersecurity infrastructure and especially in the smaller hospitals and clinics that may not have the resources and technical capabilities to institute effective data protection systems. Moreover, the enforcement of the regulations is still not unified, and a lack of specialised health data regulator, as well as duplication of authorities and absence of accountability, results in inconsistencies in compliance and accountability.[24] It is reported that the number of healthcare data breaches has been rising at a rapid pace over the past few years, and evidence shows that it has been rising by more than 50% since 2020, indicating the increased susceptibility of digital health systems.[25] Research has indicated that the cost of a healthcare data breach is higher than any other industry, as it frequently reaches USD 10 million per breach, which is very sensitive and costly healthcare information.

Table1: Insights on Patient Consent, Awareness, and Data Vulnerability in Digital Healthcare

Dimension	Key Finding (Survey Data)	%/ Range	Critical Insight
Consent Behaviour	Users accepting terms without reading	70–80%	Consent becomes procedural, not informed
Awareness Level	Users unaware of how health data is processed	65–75%	Transparency deficit in digital systems
Privacy Concern	Users worried about misuse of health data	75–85%	High anxiety despite continued usage
Consent Fatigue	Users frequently clicking "Agree" to access services	80%+	Digital design undermines meaningful choice
Data Control Rights	Users unaware of rights (access, correction, erasure)	60–70%	Weak exercise of legal protections

[24] Graham Greenleaf, India's New Data Protection Act: The Good, the Bad and the Unclear, 169 *Privacy Laws & Bus. Int'l Rep.* 1 (2023).
[25] Digital Personal Data Protection Act, supra note 8.

Trust Differential	Higher trust in government platforms vs private apps	55–60%	State seen as relatively more accountable
Experience of Data Misuse	Users reporting or suspecting misuse/breach	20–30%	Indicates real and perceived vulnerabilities
Willingness to Share Data	Users sharing data for convenience/benefits	60–70%	Trade-off between privacy and utility
Third-Party Sharing Awareness	Users unaware data is shared with third parties	65%+	Hidden data flows in digital ecosystem

Source: *Compiled from secondary surveys, industry reports, and digital health studies*

These findings demonstrate that despite the existence of consent frameworks (theoretically) and information asymmetry, consent fatigue and the awareness of users undercut these frameworks (practically), and thus the data processing in the digital health governance environment becomes less justified.

5. CRITICAL ANALYSIS: DPDP REGIME IN OPPOSITION TO PATIENT RIGHTS

5.1 Constitutional validity, Proportionality

The proportionality criterion established by the *Justice K.S. Puttaswamy v. Union of India (2017)* case needs to be applied to the constitutional validity of the Digital Personal Data Protection Act, 2023 since the law must meet the criteria of legality, necessity, and proportionality to restrict the right to privacy.[26] Although the DPDP Act meets the criteria of legality since it includes a legal framework of data processing, some issues related to the need and proportionality of particular provisions, in particular, the blanket exemptions of the State, emerge.[27] These exceptions can facilitate the access to the personal information, including sensitive health information, without any proper procedures that guarantee the safeguarding of the information, thus weakening the essence of informational privacy. Within the framework of digital healthcare, such regulatory flexibility can pose a threat to the constitutional balance

[26] *Puttaswamy*, supra note 5
[27] DPDP Act, supra note 6

between the interests of the state and individual rights, since the data is highly sensitive, and the individual dignity is closely connected with it.[28]

5.2 Failure of the Consent-Centric Model

The DPDP regime is that it is based on the idea of consent as the main principle of data processing, yet this model does not reveal considerable drawbacks in practice. Research shows that users hardly use their statutory rights, including access, correction or erasure of their personal data, a discrepancy between legal rights and their actual implementation by users. Digital consent tends to be more of a formalistic mechanism than an autonomy practice because in many cases, people are obliged to sign complicated and unfeather negotiable agreements to obtain vital healthcare.

5.3 Comparative Perspective

Another relative study also brings out the shortcomings of the Indian system. The General Data Protection Regulation (GDPR) of the European Union expressly acknowledges health data as a special category of personal data, which has an increased level of protection, as well as higher requirements regarding consent.[29] This classification takes into consideration the increased sensitivity and possibility of damage of medical information. Likewise, the United States has a sector specific approach with the Health Insurance Portability and Accountability Act (HIPAA) which offers a specific regulatory regime in the protection of health information including specifications of privacy, security and data sharing.[30] On the other hand, the DPDP Act of India is more generic sector neutral, and it is not specific in protecting the health data, which is required.[31]

5.4 Accountability and Enforcement Gaps

The success of any data protection regime is ultimately determined by the enforcement measures and in that aspect, the DPDP framework is seen to have remarkable weaknesses. The institutional capacity, independence and its abilities to manage a complex and dynamic digital ecosystem is a challenge to the Data Protection Board.[32] Additionally, no well-defined liability-system could be used to govern AI-controlled

[28] Greenleaf, supra note 28.
[29] Regulation 2016/679, General Data Protection Regulation (GDPR), art. 9 (EU).
[30] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (U.S.).
[31] World Health Organization, *Global Strategy on Digital Health 2020–2025* (2021)..
[32] Internet Freedom Foundation, *India's Data Protection Board: Governance Concerns* (2024), https://internetfreedom.in (last visited Apr. 09, 2026).

healthcare systems since it is ambiguous and could lead to injuries or discrimination in the context where automated decision-making has been conducted. International data movement also makes accountability quite challenging as health information can be handled or maintained in jurisdictions that are at varying degrees of protection, which casts doubt on jurisdiction and enforcement.[33]

6. CONCLUSION AND RECOMMENDATIONS

The Digital Personal Data Protection Act, 2023 is an important move to develop an overall data governance system in India, but its organization is still not sufficient to tackle the unique challenges of digital healthcare. The sector-neutrality nature of the Act, combined with its consent-based model does not factor in the increased sensitivity of health information and the real-world constraints of user autonomy in online setting.[34] Regardless of the constitutionality and importance of the privacy and dignity in *Puttaswamy and Common Cause case*, patient rights are rather prone to considerable losses due to the absence of enforcement, informational asymmetry, and the rise in the prevalence of data-driven healthcare platforms.

The lack of digital literacy, as well as the poor attitude of users towards data rights, and the continuation of the formalistic consent practice, affects the efficiency of the current legal regime.[35] Research shows that access and erasure are seldom exercised as a right, which points to the mismatch between legal provisions on the rights and the actual behaviour of users. When considered within the context of comparative laws like the GDPR and HIPAA, these structural vices demonstrate the weakness of an overall data protection law in protecting sensitive health data.

A multi-layered approach to reform is needed in this case. To begin with, India ought to contemplate introducing a sector-specific regime of health data protection which will offer a high level of protection to the medical information. Second, the consent model needs to be redesigned by implementing transparent, granular and intuitive systems, such as multi-language interfaces, since research indicates that simplified consent systems lead to a much better understanding of the consent.[36]

---

[33] OECD, *Cross-Border Data Flows and Privacy Protection* (2022), https://oecd.org (last visited Apr. 8, 2026).
[34] United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (2018).
[35] Centre for Internet & Society (CIS), *Digital Rights in India: User Awareness and Data Practices Survey Report* (2022), https://cis-india.org (last visited Apr. 10, 2026).
[36] OECD, Cross-Border Data Flows and Privacy Protection (2022), https://oecd.org (last visited Apr. 10, 2026).

Lastly, the future of digital healthcare must be more than just data-concentrated to patient-centred governance framework, and trust, dignity, and autonomy should be the keystones of technological transformation.

REFERENCES

1. Ministry of Health & Family Welfare, *Ayushman Bharat Digital Mission: Strategy Overview* (Gov't of India 2022).
2. NITI Aayog, *Digital Health in India: Emerging Opportunities* 12–14 (2020).
3. McKinsey & Company, *Telemedicine: A Quarter-Trillion-Dollar Post-COVID-19 Reality?* (2021).
4. Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 6–10 (Houghton Mifflin Harcourt 2013).
5. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
6. *Common Cause v. Union of India*, (2018) 5 SCC 1.
7. *X v. Principal Sec'y, Health & Fam. Welfare Dep't, Gov't of NCT of Delhi*, (2022) 10 SCC 1.
8. Digital Personal Data Protection Act, No. 22 of 2023, https://www.indiacode.nic.in/.
9. Graham Greenleaf, *India's New Data Protection Act: The Good, the Bad and the Unclear*, 169 Privacy L. & Bus. Int'l Rep. 1, 3–5 (2023).
10. *Samira Kohli v. Dr. Prabha Manchanda*, (2008) 2 SCC 1.
11. *Mr. X v. Hospital Z*, (1998) 8 SCC 296.
12. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
13. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (U.S.).
14. Regulation 2016/679 (General Data Protection Regulation), art. 9 (EU).
15. Telemedicine Practice Guidelines 2020, Ministry of Health & Family Welfare, India.

16. World Health Organization, *Global Strategy on Digital Health 2020–2025* (2021).

17. Internet Freedom Foundation, *India's Data Protection Board: Governance Concerns* (2024), https://internetfreedom.in (last visited Apr. 10, 2026).

18. Organisation for Economic Co-operation and Development, *Cross-Border Data Flows and Privacy Protection* (2022), https://oecd.org (last visited Apr. 10, 2026).

19. United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (2018).

20. Centre for Internet & Society, *Digital Rights in India: User Awareness and Data Practices Survey Report* (2022), https://cis-india.org (last visited Apr. 10, 2026).

21. IBM Security, *Cost of a Data Breach Report 2023* (2023).