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

Volume 5 | Issue 4 | 2026 Art. 03

Health Data Protection in Telemedicine and E–Health Platforms in India: A Legal Analysis of Patient Privacy

Kantipudi. Yajna Sree
Law Student, 3rd Year, BA.LL.B.,
Christ Academy Institute of Law,
Karnataka State Law University, Bengaluru

Hanshika Singh
Law Student, 3rd Year, BA.LL.B.,
Christ Academy Institute of Law,
Karnataka State Law University, Bengaluru

Recommended Citation
Kantipudi. Yajna Sree and Hanshika Singh, *Health Data Protection in Telemedicine and E–Health Platforms in India: A Legal Analysis of Patient Privacy*, 5 IJHRLR 27-42 (2026).
Available at www.ijhrlr.in/current-issues/.

Health Data Protection in Telemedicine and E–Health Platforms in India: A Legal Analysis of Patient Privacy

ABSTRACT

Digital Health refers to the growing convergences of digital technologies with healthcare delivery. The WHO has defined digital health as "a broad umbrella term encompassing eHealth, as well as emerging areas, such as the use of advanced computing sciences in 'big data', genomics and artificial intelligence". The digitization of healthcare involves two key components: the use of technology to deliver healthcare services and the digitization of medical data. The use of technology could include telemedicine, enabling patients to receive medical care without physical access to a healthcare professional or facility. Under the Drugs and Cosmetics Act, 1940 software was included as a medical device if it is used for the purposes such as a) Diagnosis, prevention, monitoring, treatment or alleviation of any disease or disorder. b) Diagnosis, monitoring, treatment, alleviation or assistance for any injury or disability. c) Investigation, replacement or modification, or support of the anatomy or of a physiological process. d) Supporting or sustaining life. e) Disinfection of medical devices. f) Control of conception. Under the Medical Devices Rules, 2017, medical devices are classified into 4 risk-based categories ranging from Class A (low risk) to Class D (high risk) which includes software in the form of digital health applications that is used for any of aforementioned purposes. The key legislations that would regulate the civil liability arising out of digital health apps are Consumer Protection Act, 2019 and Contract Act, 1872. Physicians practicing telemedicine in India are also governed by the Telemedicine Practice Guidelines, 2020 issued by the Ministry of Health and Family Welfare which provide a legal framework for registered medical practitioners to consult patients remotely via various communication platforms. The Telemedicine Guidelines prescribe some guidelines applicable specifically to data collection and processing falling within the remit of telemedicine. These guidelines essentially specify the need to maintain the confidentiality of patient data by registered medical practitioners and clarify the applicability of the IT Act and the SPDI Rules to ensure confidentiality and privacy of such data and records. The paper examines the backdrops of current laws that regulate Telemedicine and E – Health platforms as they seem to be not explicitly address telehealth and there are also significant concerns at the level of patient privacy. In this paper we would like to analyze

the legal concerns around digital health and provide an understanding of the problems these shortcomings pose, as well as policy recommendations for overcoming these problems.

KEYWORDS

Digital Health, Telemedicine, Medical Devices, Patient Data, Telemedicine Practice Guidelines

INTRODUCTION

The convergence of information technology and healthcare has given rise to what is now widely termed "digital health" a transformation accelerated significantly by the COVID-19 pandemic. In India, this shift has been particularly consequential, with the government actively promoting digital health through the Ayushman Bharat Digital Mission (ABDM)[1]. The WHO[2] defines digital health broadly to include E- Health, big data, genomics, and artificial intelligence. In practical terms, it encompasses mobile health applications, electronic health records, telemedicine platforms, wearable devices, AI-based diagnostic tools, and epidemiological analytics.

The utilization of technology within healthcare provision, management of health data, and governance of the health system is termed "digital health" in this paper. These are viewed within three dimensions, which include technology itself, the service offered, and legal/regulatory frameworks involved. An aspect of telemedicine involves patients receiving medical advice remotely through store-and-forward services, synchronous consultation services, and remote monitoring.

Such innovations come with measurable benefits including better accessibility in rural regions, reduced pressure on physical infrastructures, management support for people with chronic diseases, and valuable data for government oversight purposes. At the same time, legal questions arise related to responsibility for such platforms, regulation and governance, and the protection of health-related information. This paper aims to discuss the current state of legal and regulatory frameworks for the field of digital health in India, its key advantages and shortcomings.

LEGAL RECOGNITION OF DIGITAL HEALTH TECHNOLOGIES

In contrast to one holistic legal framework, the legal recognition of digital health technologies in India has been established through an incremental

[1] Ministry of Health & Family Welfare, Government of India, Ayushman Bharat Digital Mission: Strategy Overview (2021).
[2] World Health Organization, Global Strategy on Digital Health 2020–2025.

process through statutes, delegated legislation, and executive orders[3]. This is due to the newness of digital health technology, as well as the typical legislative lag following technological advancement[4].

The first question to arise in this context is whether software-based tools for health, including clinical decision support software, patient monitoring applications, and diagnostic algorithms, can be classified as "medical devices," which would make them subject to regulation[5]. The primary statutory framework available in India is based on the Drugs and Cosmetics Act of 1940[6], as amended. According to the Medical Devices Rules 2017 (MDR 2017)[7], the concept of a medical device is broadly defined to encompass any software designed for disease or disability detection, prevention, monitoring, treatment, or relief. Even though the notion is technology-neutral, it leaves some uncertainty regarding its scope. AI-powered radiological imaging tools fall within the purview of this definition, but wellness apps do not.

According to global models such as the EU Medical Device Regulation and the Digital Health framework of the US FDA, MDR 2017 has categorized medical devices in four classes based on risk factors; Class A to D[8]. Though a sound theoretical approach, the implementation process remains uncertain in India, especially for those that lie in between wellness, information, and clinical use.[9]

The introduction of the ABDM in 2021 has caused a further disruption in the legal regime[10]. The framework seeks to build a common digital health ecosystem that consists of Personal Health Records Application, Healthcare Professional Registry, Health Facility Registry, and Health ID per individual[11]. The collection, storage, transfer, and processing of data

[3] Ministry of Health & Family Welfare, Government of India, National Digital Health Blueprint (2019).
[4] Roger Brownsword, Law, Technology and Society: Reimagining the Regulatory Environment, 12 Law, Innovation & Tech. 1 (2020).
[5] T. K. Vishwanathan & Aparajita Lath, Regulating Digital Health in India: Issues and Challenges, 5 Indian J.L. & Tech. 67 (2019).
[6] Drugs and Cosmetics Act, 1940, No. 23 of 1940, India Code.
[7] Medical Devices Rules, 2017, G.S.R. 78(E), § 3(zb) (India).
[8] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, 2017 O.J. (L 117) 1; U.S. Food & Drug Admin., Digital Health Innovation Action Plan (2017).
[9] Shamnad Basheer & Arul George Scaria, Regulating New Technologies in India: The Case of Digital Health, 14 Indian J.L. & Tech. 23 (2018).
[10] Ministry of Health & Family Welfare, Government of India, Ayushman Bharat Digital Mission Strategy Overview (2021).
11 World Health Organization, Global Strategy on Digital Health 2020–2025 (2021).

in such a data ecosystem are guided by the ABDM Data Policy 2022[12] that encompasses ideas such as consent-based data sharing, data minimization, and purpose limitation. However, being an executive order, the policy lacks enforceability and legal bindingness since it is not a legislation. While the data governance framework of the ABDM remains legally vulnerable, it represents an important institutional move.

REGULATORY FRAMEWORK GOVERNING TELEMEDICINE

The Ministry of Health and Family Welfare's Telemedicine Practice Guidelines, 2020 (TPG 2020) significantly influenced telemedicine regulations in India[13]. When combined with the National Medical Commission Act of 2020[14], these principles make up the first thorough framework that addresses telemedicine practice.

The Registered Medical Practitioners are allowed to perform their consultations through emails, SMS, video, and voice calls according to TPG 2020. They are responsible for setting standards related to patient identification and verification, prescription regulations, restrictions of Schedule X drugs, safety of sensitive individuals, confidentiality, and documentation. Collectively, these clauses clearly recognize telemedicine as an authentic form of medical practice under Indian law[15].

Further, TPG 2020 states that telemedicine information falls under the ambit of the SPDI Rules, 2011 and the Information Technology Act, 2000[16]. However, no new obligations are created by either legislation that goes above and beyond the existing standards. Hence, the legal protection of telemedicine information can only be achieved through a more robust set of laws than currently exist.

The National Medical Commission has been established by the NMC Act, 2020[17] as the apex regulatory body overseeing medical practice and training. Breaches of TPG 2020 can be referred to the Ethics and Medical Registration Board (EMRB) as cases of professional misconduct. However, such reporting is more of an issue of discipline than that of privacy. Processes tend to be lengthy and inappropriate to use when seeking compensation from affected individuals whose personal health

12 National Health Authority, Government of India, ABDM Health Data Management Policy (2022).
13 Board of Governors in Supersession of Medical Council of India, Telemedicine Practice Guidelines (2020).
14 National Medical Commission Act, 2019, No. 30 of 2019, India Code.
15 Telemedicine Practice Guidelines, supra note 1.
16 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India); Information Technology Act, 2000, No. 21 of 2000, India Code.
17 National Medical Commission Act, supra note 2.

data had been mishandled. These challenges are even amplified by the cross-jurisdictional nature of telemedicine.

Regulatory challenges become even greater when one takes into consideration the rising application of artificial intelligence and machine intelligence in telemedicine applications. Clinical decision support software, diagnostic technologies, and symptom-checking algorithms raise difficult questions about their classification, validation, liability, and accountability in case of patient harm. Existing regulations, including the NMC Act, TPG 2020, and MDR 2017, do not provide any guidelines regarding the need for accountability and transparency in algorithmic design and operation. Moreover, no mention is made of the legal status of AI applications used for telemedicine purposes under existing regulations[18].

DATA PROTECTION AND PRIVACY LAWS APPLICABLE TO HEALTH DATA

Health information is one of the most delicate categories of personal data. Health data include medical records, test results, prescription history, genetic data, and psychological data. The risk of discrimination, stigma, and gross violations of human autonomy and dignity could arise from any unauthorized disclosure or exploitation of such data. Despite this, India has been long lacking an information regulation regime that specifically caters to protecting health information online.[19]

The IT Act 2000 and the SPDI Rules 2011 were the key statutes that regulated health data protection before the enactment of the DPDP Act 2023[20]. The body corporates that negligently process SPDI and result in wrongful gain or loss to any person are liable under Section 43A of the IT Act[21]. Health data falls within the ambit of SPDI as per the SPDI Rules and impose basic obligations on the processing of health data. However, there are four major limitations with these rules.

In the first place, while the public sector has a great role to play in healthcare delivery in India, the scope is limited to body corporates and does not cover government bodies, public hospitals, and non-profit healthcare institutions. Secondly, especially within the hospital setting where the individual seeking care may be vulnerable, the rules

[18] U.S. Food & Drug Admin., Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan (2021).
[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India)
[20] Information Technology Act, 2000, No. 21 of 2000, India Code; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[21] Information Technology Act, 2000, § 43A (India).

concerning consent are poorly formulated and do not provide for the doctrine of informed consent. Thirdly, it is unfortunate that the already overstretched adjudicatory process of the IT Act has been made responsible for implementing the Rules which do not have a dedicated body to oversee data protection.

The DPDP Act of 2023 represents a significant leap forward[22]. The law establishes a system of rights relating to the processing of digital personal data not only in India but also the processing outside India involving the profiling of individuals who are Indian citizens. In terms of healthcare, such rights take on added significance. Rights include accessing details about the processing, right to correction and deletion, grievances, and appointment of a representative in case of incompetence or death.

However, the Act is accompanied by some important limitations. First, the Act does not create any particular classification of "sensitive personal data," unlike the GDPR and SPDI Rules. Rather, the general requirements of the Act apply to health data, as opposed to a more stringent regime of enhanced protection. Second, the Act provides a substantial number of exemptions for instrumentalities of the state, which means that the government's health organizations can process health data without obtaining consent, based on reasons of public health. This requirement has attracted much criticism due to possible privacy violations.

A further concern is that the DPDP Act had not been fully operationalised as of early 2024. The rules necessary to implement the Act, including those constituting the Data Protection Board of India, had not been notified. This creates a continuing institutional and legal gap.

Beyond the DPDP Act and SPDI Rules, sector-specific norms also govern health data. The Clinical Establishments (Registration and Regulation) Act, 2010 requires clinical establishments to maintain and protect patient records[23]. The NMC's Ethics Regulations impose professional duties of confidentiality on RMPs. The Pharmacy Practice Regulations, 2015 impose similar obligations on pharmacists. While these rules are important, their primary focus remains professional ethics and recordkeeping rather than the comprehensive recognition and enforcement of patient data rights in a digitally connected healthcare environment.

[22] Digital Personal Data Protection Act, 2023, No. 22 of 2023, India Code.
[23] Clinical Establishments (Registration and Regulation) Act, 2010, No. 23 of 2010, India Code.

PRIVACY CONCERNS IN TELEMEDICINE AND E–HEALTH

The importance of privacy was acknowledged as far back as the time of the Hippocratic Oath.[24] Both consequentialist and deontological ethical justifications exist for protecting privacy in the patient–provider relationship.[25] This is essential, given the fiduciary nature of the doctor-patient relationship and the mutual expectations of trust between patient and doctor. Privacy in healthcare has many facets, including informational privacy, physical privacy, associational privacy, proprietary privacy and decisional privacy.[26] The issue ofprivacy in healthcare came up in India in the 1998 case of Mr X vs Hospital A. Mr X was found to be HIV+ when he donated blood. The allegedly unauthorized disclosure of his HIV+ status by the hospital[27] resulted in Mr X's marriage being called off, leading him to seek legal redress. The court held that doctors must maintain secrecy about their patients.

Health privacy is vital as data can be misused in multiple ways by employers, governments, and other third parties to treat individuals differently while providing services, benefits, and employment.[28] For instance, unauthorized access to health data can harm individuals suffering from stigmatized diseases, as also those with mental health problems. Cybercriminals can breach the security of health data to blackmail individuals or indulge in identity theft.[29] Violations of privacy in the healthcare sector in India include healthcare providers not specifying the purpose of collecting data, collecting more health data than required for processing, sharing health data for research without de – identification and anonymisation, revealing health information to third parties without consent, lack of security safeguards for health data resulting in breach of data confidentiality, and not informing the data

[24]Arenas A, translator. Hippocrates' Oath. Boston University website. Available from: https://www.bu.edu/arion/files/2010/03/Arenas_05Feb2010_Layout-3.pdf

[25] Jain D. Regulation of Digital Healthcare in India: Ethical and Legal Challenges. *Healthcare (Basel).* 2023 Mar 21; 11(6):911. https://doi.org/10.3390%2Fhealthcare11060911

[26] Mani T. Privacy in Healthcare: Policy Guide. Centre for Internet and Society. Centre for Internet and Society website. 2014 Aug 26. Available from: https://editors.cis-india.org/internet-governance/blog/privacy-healthcare.pdf

[27] Supreme Court of India. Mr X v Hospital Z. Appeal (Civil) 4641 of 1998. 1998 Sep 1. Available from: https://indiankanoon.org/doc/382721/

[28] Gaba J M, Estremadura J M. Data protection of biometric data and genetic data. Ateneo Law Journal. 2020[Cited 2023 Oct 10]; 64(3):949-982. Available from: https://heinonline.org/HOL/P?h=hein.journals/ateno64&i=956

[29] Determann L. Healthy data protection. Mich Telecom Tech L Rev. 2020; 26(2): 229-278. https://repository.law.umich.edu/mtlr/vol26/iss2/3?utm_source=repository.law.umich.edu%2Fmtlr%2Fvol26%2Fiss2%2F3&utm_medium=PDF&utm_campaign=PDF.

principal in case of data breach.[30] These concerns are exacerbated by the high illiteracy rate, lack of privacy awareness, and questionable informed consent in India. People may not understand the privacy implications of their health data, especially when using online services.

Privacy issues in healthcare are gaining huge significance because of the increasing collection of individuals health data, such as through the Internet of Medical Things, including wearbles such as fitness watches.[31] There has also been a proliferation of mobile applications and websites for telemedicine, counseling, wellness, and sale of medicines that collect health data. Big Medical Data is analysed using artificial intelligence and data mining and matching techniques to generate new medical insights.[32] This means a person's helath information is now increasingly available to various third parties outside the doctor – patient relationship, with the possibility of privacy harm including loss of reputation or humiliation, discriminatory treatment, blackmail or extortion, mental injury, denial or withdrawal of services, and restrictions on speech for fear of being observed or suveilled.[33]

The risks associated with inadequate data protection in telemedicine are multifaceted:

- **Data breaches**: Cybersecurity threats pose significant risks to the confidentiality and integrity of patient data. Data breaches can occur due to hacking, inadequate security measures, or human error, leading to unauthorized access to sensitive information.

- **Identity Theft and Fraud**: The misuse of personal health data can result in identity theft, insurance fraud, and other criminal activities. Patients whose data is compromised may face financial losses and long – term repercussions on their credit and personal safety[34].

- **Erosion of Trust**: Trust is fundamental to patient – provider relationship.[35] When patients are concerned about the security of

[30] Id 3
[31] Id 5
[32] Rajaretnam T. Data mining and data matching: Regulatory and ethical considerations relating to privacy and confidentiality in medical data. *J* Int Commer Law Technol. 2014 Jan; 9(4):294-310.
[33] Ministry of Law and Justice, Govt of India. The Personal Data Protection Bill, 2019. Bill No. 373 0f 2019[Cited 2023 Oct 10]. Available from: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[34] Sacitha. K, Dr. M.S. Sharmila(2025), Telemedicine and Consumer Protection Ensuring Patient Privacy and Safety in a Digital Healthcare Landscape, Journal of Neonatal Surgery, 2226-0439, vol.14, Issue 7.
[35] Greenhalgh, T., et al. (2020). Privacy and Trust in Telehealth. British Medical Journal

their personal information, they may be less likely to engage in telemedicine services. This reluctance can hinder the effectiveness of telehealth initiatives, ultimately impacting patient outcomes.

- **Legal and Financial Liabilities:** Helathcare provides and organizations face significant legal and financial repercussions in the event of a data breach. Without robust legal frameworks, these entities may be ill – prepared to address the complexities of data protection and may incur substantial penalties.[36]

An examination of the data practices of India's leading health-tech platforms reveals the practical dimensions of the regulatory deficit. Practo, India's largest digital health platform with over 25 million monthly users, collects consultation records, prescription data, health records uploaded by users, appointment histories, and insurance information through its unified platform.[37] Its privacy policy permits data sharing with 'partners' for 'improving services' — language sufficiently vague to encompass a wide range of secondary uses. The platform 1mg (now Tata 1mg following acquisition by Tata Digital), which combines teleconsultation, e-pharmacy, and diagnostic services, collects health data across all three verticals and its privacy policy permits processing for 'analytics,' 'research,' and 'personalisation' purposes.[38] Apollo 24|7, the digital health arm of the Apollo Hospitals Group, integrates teleconsultation with its hospital network, pharmacy chain, and diagnostic centres, creating an unprecedented data aggregation capability spanning both digital and physical healthcare interactions. Tata Health similarly leverages the Tata Group's conglomerate structure to connect health data with broader consumer data ecosystems.

The intersection of telemedicine data with the insurance sector raises particularly acute concerns that India's regulatory framework fails to address. The Insurance Regulatory and Development Authority of India (IRDAI) has progressively encouraged the digitisation of insurance underwriting and claims processes, including the use of electronic health records for risk assessment.[39] When a patient's telemedicine consultation data — including diagnoses, prescriptions, and even the frequency of consultations — is accessible to insurers, the potential for adverse underwriting decisions based on health data is significant. A patient who

(BMJ), 368, m998.DOI: 10.1136/bmj.m998.

[36] Taylor, A .(2021). Data Protection and Tele-health: Addressing Legal Challenges. International Journal of Law and Information Technology, 29(2), 225-242

[37] Practo. (2024). Privacy policy. Bangalore: Practo Technologies Pvt. Ltd.

[38] Tata 1mg. (2024). Privacy policy. Gurugram: Tata 1mg Healthcare Solutions Pvt. Ltd.

[39] Insurance Regulatory and Development Authority of India. (2022). Guidelines on information and cybersecurity for insurers. Hyderabad: IRDAI.

seeks a teleconsultation for a mental health concern, for example, may face higher premiums or denial of coverage if that data is shared with or accessible to insurance underwriters. Under India's DPDP Act, no specific restriction prevents the use of telemedicine-derived health data for insurance underwriting, provided that a general consent was obtained at the time of data collection. The IRDAI's data protection guidelines, while requiring insurers to maintain data confidentiality, do not specifically address the acquisition and use of telemedicine-derived health data and lack the statutory force of the DPDP Act.[40]

GAPS IN EXISTING LEGAL FRAMEWORK

India's Digital Personal Data Protection Act 2023, which received Presidential assent on 11 August 2023, represents the culmination of a legislative journey spanning nearly a decade, from the Justice B.N. Srikrishna Committee Report of 2018 through successive draft bills.[41] The Act applies to the processing of digital personal data within India and to processing outside India in connection with offering goods or services to data principals in India. It establishes the rights of data principals (notice, consent, access, correction, erasure, grievance redressal, nomination) and the obligations of data fiduciaries (purpose limitation, data minimisation, accuracy, storage limitation, security safeguards). The most significant omission in the DPDP Act, from a health data perspective, is the absence of any special category or sensitive personal data classification. The Act's predecessor, the Personal Data Protection Bill 2019, had included "health data" in its definition of sensitive personal data under Clause 3(36), subjecting it to additional processing conditions including explicit consent and purpose limitation.[42] This provision was removed in the subsequent iterations, and the enacted DPDP Act treats all personal data uniformly, regardless of sensitivity. The Act's Section 4 requires consent for all personal data processing and Section 6 specifies requirements for valid consent (free, specific, informed, unconditional, unambiguous, with clear affirmative action), but these apply identically to a user's name and to their HIV status or psychiatric diagnosis.

This uniform treatment creates several specific vulnerabilities in the telemedicine context. First, the consent framework does not require explicit or heightened consent for health data processing, unlike GDPR Article 9(2)(a) which requires consent that is "explicit" for special category data — a higher threshold than the standard "unambiguous" consent under Article 6. Second, the Act does not mandate Data

[40] Id 16.

[41] Parliament of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India

[42] Ministry of Electronics and Information Technology. (2019). Personal Data Protection Bill, 2019. New Delhi: Government of India.

Protection Impact Assessments for health data processing, unlike GDPR Article 35(3)(b) which specifically identifies large-scale processing of special category data as triggering a mandatory DPIA. Third, the Act's exemptions under Section 17 — which allow government processing without consent for specified purposes — are not subject to additional safeguards when applied to health data. Fourth, the penalty framework under Section 33, while providing for penalties up to 250 crore rupees, does not differentiate between breaches involving health data and breaches involving less sensitive data categories.[43] The implications of this gap are amplified by the architecture of India's digital health ecosystem. The Ayushman Bharat Digital Mission (ABDM), launched in 2021, aims to create a unified health data infrastructure through the Ayushman Bharat Health Account (ABHA), health information exchanges, and interoperable electronic health records. By 2024, over 550 million ABHA numbers had been generated.[44] The ABDM's Health Data Management Policy (HDMP) attempts to fill the legislative gap through administrative guidelines, establishing consent-based data sharing, purpose limitation, and security requirements (NHA, 2022). However, as administrative policy rather than legislation, the HDMP lacks statutory enforceability, cannot override the DPDP Act's provisions, and is not subject to the penalty framework applicable to statutory violations.

The Supreme Court's landmark decision in Puttaswamy (2017) recognized informational privacy as a facet of the fundamental right to privacy under Article 21 and established the proportionality test for privacy restrictions: legality, legitimate aim, proportionality, and procedural safeguards. The Court specifically identified health data as among the most intimate categories of personal information, with Justice Chandrachud observing that medical records relate to the "most intimate aspects of personal life".[45] The DPDP Act's failure to operationalize this judicial recognition through special category classification arguably falls short of the constitutional mandate articulated in Puttaswamy.

The contrast between the DPDP Act 2023 and its intellectual predecessor — the Justice B.N. Srikrishna Committee Report of 2018, titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' — is instructive in understanding what protections were deliberately omitted. The Srikrishna Committee explicitly recommended that certain categories of personal data, including health data, genetic data, biometric data, official identifiers, sexual orientation, caste, religious beliefs, and

[43] Parliament of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India.
[44] National Health Authority. (2024). Ayushman Bharat Digital Mission: Progress report. New Delhi: NHA.
[45] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, para 169.

financial data, be classified as 'sensitive personal data' subject to enhanced processing conditions.[46] The Committee's rationale was grounded in the recognition that these data categories, if misused, pose heightened risks of discrimination, social exclusion, and psychological harm. For health data specifically, the Committee noted that disclosure of medical conditions such as HIV/AIDS, mental illness, or reproductive health information could result in severe social stigma in the Indian context.

The Srikrishna Committee recommended several specific protections for sensitive personal data that did not survive into the enacted DPDP Act: (a) processing only on the basis of explicit consent, defined more stringently than ordinary consent; (b) mandatory Data Protection Impact Assessments before initiating processing of sensitive data at scale; (c) restrictions on cross-border transfer of sensitive personal data, requiring that such data be stored on servers located in India (data localisation); (d) a higher standard of purpose limitation, requiring that sensitive data collected for one purpose not be processed for any materially different purpose without fresh consent; and (e) enhanced breach notification obligations, including shorter timelines and mandatory notification to affected individuals.[47] The Personal Data Protection Bill 2019, which was the legislative translation of the Committee's recommendations, incorporated many of these provisions under Clause 3(36) and Chapter III. The subsequent withdrawal of the 2019 Bill and its replacement by the DPDP Act 2023, which excised the entire sensitive data framework, represents a significant regression from the considered recommendations of the expert committee appointed by the Government itself[48].

POLICY RECOMMENDATIONS AND REFORMS

Based on the analysis, this paper proposes reforms to address India's health data protection:

1. Transparency, data confidentiality, and cyber security must be addressed in the guidelines concerning the health data of individuals to be used by medical software (third parties), and this must have a transparent data sharing agreement with the rights of patients being protected.[49] Scholars argue for the pressing need

[46] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. New Delhi: Ministry of Electronics and Information Technology.
[47] Id 19
[48] Varsha P, Dr. Ch. Venkateswarlu, Health Data Protection: A Comparative Analysis of Telemedicine Data Protection Framework in Global Scenario, International Journal for Multidisciplinary Research, Volume 8, Issue 2, March – April 2026.
[49] Ranganathan S. Towards a Holistic Digital Health Ecosystem in India. Observer

for a rights-based framework in the use of data and ownership of the data.[50]

2. the issue of liability must be addressed. Shoshana Zuboff terms this era as one of "surveillance capitalism", which is a legitimate concern regarding the usage and processing of individual, community, and societal data.[51]
3. Identifiable health data should be used only for the limited purpose of providing a healthcare service and its commercial use should not be permitted. There should be a timebound requirement for carrying out data protection impact assessments for healthcare providers. Privacy should be protected by design, strict penalties should be imposed for violations of health data protection provisions, and there must be high compensation for breach of health data privacy.
4. The most direct reform is the introduction of a "special category" or "sensitive personal data" classification within the DPDP Act through amendment. Health data, biometric data, genetic data, data revealing racial or ethnic origin, and data concerning sexual orientation should be classified as sensitive personal data subject to enhanced protections: explicit consent requirements, mandatory Data Protection Impact Assessments, heightened security obligations, restricted automated decision-making, and enhanced breach notification timelines. This approach is consistent with the original intent of the PDP Bill 2019, which included such classification before its removal.
5. Given that the DPDP Act amendment process may be protracted, a complementary approach is the enactment of sector-specific health data governance legislation — an "Indian Health Data Protection Act" modelled on Health Insurace Portability and Accountability Act of 1996 (HIPAA) sector-specific approach but incorporating GDPR-standard protections. Such legislation would define the categories of entities subject to health data obligations (healthcare providers, telemedicine platforms, health information exchanges, e-pharmacies, health insurers, health data processors), establish minimum security standards for electronic

Research Foundation. Apr 2, 2020. Available online: https://www.orfonline.org/research/towards-a-holistic-digital-health-ecosystem-in-india-63993/?amp

[50] Tisne M. It's Time for a Bill of Data Rights. MIT Technology Review. Dec 14, 2018. Available online: https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/

[51] Bridle J. The Age of Surveillance Capitalism by Shoshana Zuboff Review—We Are the Pawns. The Guardian. Feb 2, 2019. Available online: https://www.theguardian.com/books/2019/feb/02/age-of-surveillance-capitalism-shoshana-zuboff-review

health data, create health-data-specific consent requirements, mandate interoperability standards, and establish enforcement mechanisms.

6. Neither the DPDP Act's Data Protection Board nor the National Health Authority currently possesses the combined health-sector expertise and data protection enforcement capacity needed for effective health data governance. A specialised Health Data Protection Authority — either as an independent body or as a specialised division within the Data Protection Board with health-sector expertise — should be established. The UK's Caldicott Guardian model provides a useful template: requiring every healthcare organisation, including telemedicine platforms, to designate a senior official responsible for health data governance would create distributed accountability within the centralised regulatory framework.
7. The Ayushman Bharat Digital Mission's Health Data Management Policy should be elevated from administrative guidelines to legally enforceable standards. Additionally, all telemedicine platforms should be required to undergo health data governance assessment analogous to the UK's Digital Technology Assessment Criteria (DTAC) before being permitted to operate. This assessment should cover data minimisation practices, consent management, encryption standards, access controls, audit logging, data retention policies, cross-border data transfer safeguards, and incident response capabilities. Compliance should be a condition for registration under the Clinical Establishments Act 2010 or any future National Telemedicine Act[52].

CONCLUSION

The digitization of healthcare has the potential to increase accessibility to quality healthcare in India, which could greatly benefit marginalized individuals and communities. However, the legal and ethical challenges to implementing it must be addressed along with other structural challenges. Digitally aware healthcare workers are essential when conducting tests or administering procedures, including household health screenings, but the infrastructure of the country also needs to adapt to support digital health solutions. India's telemedicine ecosystem processes health data at an unprecedented scale — over 550 million ABHA registrations, 150 million eSanjeevani consultations, and millions of private platform interactions annually. This data traverses vertically integrated platforms that aggregate teleconsultation records, prescription histories, diagnostic results, and insurance claims without

[52] Id 25.

any health-data-specific governance obligations. The ABDM's administrative guidelines, while well-intentioned, cannot substitute for legislative protections with statutory enforceability. The Supreme Court in Puttaswamy recognised health data as among the most intimate categories of personal information and established the constitutional framework for its protection. The DPDP Act's failure to translate this constitutional mandate into statutory protections is not merely a legislative gap but a potential constitutional deficiency. India's digital health transformation cannot be built on a data protection framework that fails to recognise the fundamental difference between a patient's medical diagnosis and their shopping preferences.