WORKING PAPER

December 2025

When Healthcare Meets Big Data

An Analysis of Privacy Policies and Third-Party Data Flows in Telemedicine Platforms in India

A Working Paper

C-HELP | CENTRE FOR HEALTH EQUITY, LAW & POLICY

ILS

Working Paper
When Healthcare Meets Big Data: An Analysis of Privacy Policies and Third-party Data Flows in Telemedicine Platforms in India

December 2025

The Centre for Health Equity, Law & Policy is a research, knowledge production and advocacy forum, which works on law & policy issues related to health, embedding its work in the right to health as envisaged within India's constitutional framework and her international commitments.

Authors
Shivangi Rai, Shefali Malhotra, Arnav Mahurkar

Contact Information
contact@c-help.org

Centre for Health Equity, Law & Policy
Indian Law Society
Law College Road
Pune 411004
Maharashtra, India

Table of Contents

1 Introduction

Telemedicine in India has undergone a significant transformation, particularly since the COVID-19 pandemic - from a niche service to a mainstream mode of healthcare delivery. Yet, alongside this growth, concerns have mounted over the privacy and governance of individuals' sensitive health data collected and processed on telemedicine platforms.

Globally, critics have consistently pointed to vague privacy policies, bundled consent mechanisms, opaque third-party data sharing and the heavy reliance on Big Tech infrastructure by web and mobile health applications. In India, however, to the best of our knowledge, research on privacy and data security practices of these platforms remains limited. In particular, what has been missing is a comprehensive analysis that examines both the legal adequacy of privacy policies and the technical realities of third-party data flows in telemedicine platforms.

The present paper fills this gap by evaluating privacy policies against international and domestic legal frameworks, while also tracking third-party data flows using technical tools to reveal what, how and where personal information is shared on nine telemedicine web platforms. The research is guided by two central questions: to what extent do the privacy policies of these platforms comply with globally recognised consent and disclosure standards? And, how do their actual data-sharing practices align with the notice, consent, and privacy requirements of the Digital Personal Data Protection Act 2023 (DPDPA)?

The legal analysis benchmarked privacy policies against international data protection legal frameworks from the European Union, the United States, Brazil, Nigeria, Thailand and India. The parameters of analysis were organised under four heads: notice and consent, privacy principles, user rights, and transparency and accountability. The technical analysis simulated user journeys across teleconsultation, e-pharmacy, and diagnostic pathways, using network inspection tools to capture real-time data flows and identify third-party sharing.

The findings reveal systematic deficiencies across the platforms. First, privacy policies were typically buried in website footers, available only in English, and presented in ways that implied consent through browsing and continued use rather than requiring explicit opt-in consent, with an affirmative action. None of the platforms offered granular consent, and only limited technical permissions, such as camera or location access, were subject to user choice.

Second, data collection was extensive and included sensitive demographic attributes such as religion, ethnicity and marital status. All commercial platforms collected device and usage data via first and third-party cookies and trackers, enabling profiling and potentially device fingerprinting. The stated purposes for processing bundled core healthcare functions with vague categories such as 'business purposes' or 'product improvement'.

Third, third-party data sharing was pervasive. All commercial platforms shared data with external entities for analytics, advertising and marketing, with common recipients including Google, Microsoft and Meta. Some, such as Practo and PharmEasy, stated that they sell de-identified data, while MediBuddy shared information with employers. Only Netmeds

provided a cookie consent banner, and even that was limited. Privacy principles, such as purpose limitation and data minimisation, were routinely violated, with platforms collecting far more data than necessary and retaining anonymised data indefinitely. Security assurances were vague, with few specifics on encryption or firewalls, and accuracy was left to users to maintain.

Fourth, user rights were inconsistently recognised. While some platforms acknowledged rights to access, erasure, and rectification, none recognised rights related to automated decision-making, data portability, or nomination. Mechanisms for exercising rights were weak, often limited to generic email addresses with no clear process laid out.

Fifth, transparency and accountability were similarly lacking. Only three out of the nine platforms disclosed cross-border transfers. Contact details for data protection officers or grievance officers were inconsistently provided. In some cases, one individual held both the roles. No platform committed to notifying users of policy updates or breaches.

Taken together, these findings highlight systemic gaps: consent that is implied and tokenistic, rather than substantive; excessive and unnecessary data collection; opaque third-party data sharing that entrenches Big Tech dominance with implications for competition and innovation; vague privacy policy language that obscures actual practices, and incomplete recognition of users' digital rights. These deficiencies are compounded by the limitations of the DPDPA that weakens notice obligation, omits key digital rights, and fails to mandate privacy policies as distinct from notice for consent, altogether. Even full compliance with the 2023 Act would therefore leave users vulnerable.

This study offers the first integrated legal and technical assessment of Indian telemedicine web platforms, benchmarking them against both global best practices and domestic legal standards, as well as highlighting the urgent need for reform in the sector. The paper is organised as follows: Section 2 provides the background; Section 3 articulates the research objectives; Section 4 explains the methodology; Section 5 presents detailed findings; Section 6 discusses the implications of these findings; and Section 7 concludes by making recommendations.

2 Background

India has witnessed a steady increase in telehealth services in the past decade, expanding from USD 85 million in 2010 to USD 1 billion in 2020.[1] However, it was the COVID-19 pandemic that ushered in a world of physical distancing and remote interactions and propelled telemedicine platforms into the mainstream.[2] In 2024, the Indian market was valued

[1] Ernst & Young and Indian Pharmaceutical Alliance, *Healthcare Goes Mobile: Evolution of Teleconsultation and e-Pharmacy in New Normal*, August 2020.
[2] Soumen Mandal, "Why Telemedicine Is The Next Big Opportunity In Indian Healthtech" *Inc42 Media*, 16 April 2020.

at USD 3.1 billion, and is projected to grow at a compound annual growth rate of 20.5% between 2025-2033, reaching USD 19.90 billion by the end of this period.[3]

Even as telemedicine platforms continue to grow in scale and visibility in India, they have been criticised for their loose privacy policies, opaque security practices, misuse of sensitive personal information for commercial gain and a lack of regulatory oversight.[4] Of these critiques, privacy and data governance practices of mobile and web health applications have found resonance in global research, revealing recurring patterns including inadequate privacy policy disclosures, broad "take it or leave it" consent terms, routine undisclosed third-party sharing for data monetisation, profiling and targeted advertisement, and structural reliance on cloud services and infrastructure controlled by Big Tech.[5]

However, few studies within the Indian context have substantively explored this issue. The earliest of these is a 2017 study that examined the privacy policies of 30 applications, which were classified under the 'medical category' on Google Play and App Store in India.[6] The analysis raised concerns around data deletion and encryption, concluding that developers had

---

[3] IMARC Group, *India Telemedicine Market Size, Share, Trends and Forecast by Component, Type, Deployment Mode, Modality, Application, End User, and Region, 2025-2033*.

[4] Mihir Dalal, "Why telemedicine needs an urgent fix" *Livemint*, 26 August 2020; Pradeep Pankajakshan Nair et al., "Video teleconsultation services for persons with epilepsy during COVID-19 pandemic: An exploratory study from public tertiary care hospital in Southern India on feasibility, satisfaction, and effectiveness," 117 *Epilepsy & Behavior* 107863 (2021); U. Venkatesh, Gandhi P. Aravind and Anbu Ananthan Velmurugan, "Telemedicine practice guidelines in India: Global implications in the wake of the COVID‐19 pandemic," 14 *World Medical & Health Policy* 589–99 (2022); Alison C. Dcruz et al., "The rise of E-pharmacy in India: Benefits, challenges, and the road ahead," 54 *Indian Journal of Pharmacology* 282–91 (2022); Department-related Parliamentary Standing Committee on Commerce, *Promotion and Regulation of E-Commerce in India* (Rajya Sabha Secretariat, Parliament of India, New Delhi, 21 July 2022); Dipika Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," 11 *Healthcare* 911 (2023); Aparna Venkataraman et al., "Facilitators and Barriers for Telemedicine Systems in India from Multiple Stakeholder Perspectives and Settings: A Systematic Review," 30 *Telemedicine and e-Health* 1341–56 (2024); Ashish Srivastava, "Chemist body calls for scrutiny of e-pharmacy ops amid fake drug busts" *The New Indian Express*, 30 July 2025.

[5] Several international studies have delved into scrutinizing the privacy and security practices of digital health platforms globally. They have shed light on data exploitation while highlighting the risks in mHealth apps, emphasizing transparency issues and the lack of privacy policies. Investigations into medicines-related mobile apps underscored routine data sharing without adequate transparency and have exposed significant privacy problems, urging caution. Reviews of mHealth apps reveal alarming deficiencies in data privacy, sharing, and security practices. See, Tobias Dehling et al., "Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android," 3 *JMIR mHealth and uHealth* e8 (2015); Ali Sunyaev et al., "Availability and quality of mobile health app privacy policies," 22 *Journal of the American Medical Informatics Association* e28–33 (2015); Privacy International, "REPORT: Your mental health for sale," 2019*available at*: http://privacyinternational.org/node/3193 (last visited July 16, 2025); Quinn Grundy et al., "Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis" *BMJ* l920 (2019); Leysan Nurgalieva, David O'Callaghan and Gavin Doherty, "Security and Privacy of mHealth Applications: A Scoping Review," 8 *IEEE Access* 104247–68 (2020); Razieh Nokhbeh Zaeem and K. Suzanne Barber, "Comparing Privacy Policies of Government Agencies and Companies: A Study using Machine-learning-based Privacy Policy Analysis Tools," 2021; Gioacchino Tangari et al., "Mobile health and privacy: cross sectional study" *BMJ* n1248 (2021); Najd Alfawzan et al., "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis," 10 *JMIR mHealth and uHealth* e33735 (2022); Kaijun Liu et al., "Evaluating the Privacy Policy of Android Apps: A Privacy Policy Compliance Study for Popular Apps in China and Europe," 2022, in Z. Liu (ed.), *Scientific Programming* 1–15 (2022).

[6] Brinda Hansraj Sampat and Bala Prabhakar, "Privacy Risks and Security Threats in mHealth apps," 26 *Journal of International Technology and Information Management* 126–53 (2017).

not prioritised data security and transparency. Another 2021 study, based in Tamil Nadu, highlighted that there was no way for users to determine if application developers in India have implemented sufficient security measures to protect patient data and their mobile health applications from malicious attacks.[7] Most recently, a 2023 study by the Centre for Internet and Society and Privacy International examined third-party data sharing practices of nine Indian web and mobile health applications.[8] The findings revealed significant gaps in transparency and a lack of meaningful informed consent in how user data is shared with third-party entities.

We add to this line of literature by conducting a legal analysis of the privacy policies and technical analysis of third-party data sharing practices of major telemedicine web platforms operating in India. Our study is distinct in three aspects. To begin with, it is the first in the Indian context to examine the text of the privacy policies and actual data flow practices in tandem. In addition, unlike prior research, we benchmark our analysis not only against global best practices but also against India's DPDPA. Finally, while existing studies have typically examined general health, wellness and fitness apps, we focus solely on telemedicine platforms offering core healthcare services, including doctor consultation, e-pharmacy and/or diagnostic services.

Given the Indian government's push towards digitalisation of the health sector through the Ayushman Bharat Digital Mission (ABDM) and the rapid expansion of the telemedicine market in recent years, the study is important as it reveals information on the inner workings of telemedicine web platforms, accessed by an ever-increasing number of Indians. The study also contains important findings and recommendations which are relevant to the DPDPA and accompanying rules, as well as their implementation.

3 Research objective and questions

This study critically examines how telemedicine web platforms in India govern the processing[9] of patient data, through a legal and technical analysis of their privacy policies and data flow practices, respectively. Drawing on the definition of telemedicine[10] articulated in the Telemedicine Practice Guidelines 2020, which emphasises the role of digital technologies

[7] Pradeep Pankajakshan Nair et al., "Video teleconsultation services for persons with epilepsy during COVID-19 pandemic: An exploratory study from public tertiary care hospital in Southern India on feasibility, satisfaction, and effectiveness," 117 *Epilepsy & Behavior* 107863 (2021).

[8] Privacy International and Centre for Internet and Society, "The hidden cost of digital health services"*available at*: http://privacyinternational.org/long-read/5151/hidden-cost-digital-health-services (last visited July 16, 2025).

[9] "Processing in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction." See, Government of India, *Digital Personal Data Protection Act*, 2023, s. 2(x).

[10] Telemedicine is defined as "the delivery of health care services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities." See, Ministry of Health and Family Welfare, Telemedicine Practice Guidelines, 2020, guideline XX.

in delivering health care across distance, we focus on nine web platforms offering doctor-patient consultations, e-pharmacy and/or diagnostic services. Specifically, we investigate:

1. To what extent do the privacy policies of selected telemedicine web platforms in India comply with the globally recognised consent and disclosure practices as reflected in our framework of analysis?

2. Are the selected telemedicine web platforms in India facilitating third-party data sharing, and how do these practices align with the notice, consent and privacy requirements under the DPDPA?

4 Methodology

For this study, we selected nine telemedicine web platforms operating in India that offer a combination of teleconsultation, e-pharmacy and diagnostic services. The selection includes eight commercial platforms - Practo, Tata 1MG, Lybrate, Apollo 24/7, MediBuddy, Netmeds, PharmEasy and MedPlusMart, and one public initiative, *eSanjeevani*, India's national telemedicine platform developed by the Ministry of Health and Family Welfare. We downloaded the privacy policies of the selected platforms from their respective websites.

Next, we developed a legal analysis framework to examine the aforementioned privacy policies. Our framework is grounded in the Universal Declaration of Human Rights (UDHR) and the International Covenant for Civil and Political Rights (ICCPR), both of which recognise the human right to privacy.[11] Additionally, we approach the right to privacy as an integral part of the right to health as recognised under the International Covenant on Economic, Social and Cultural Rights (ICESCR)[12] and normatively substantiated by the General Comment No. 14.[13] We also anchor our approach in the Indian Supreme Court's landmark ruling in Justice K.S.Puttaswamy vs Union, which unequivocally reaffirmed the right to privacy as a fundamental right under Articles 14, 19 and 21 of the Constitution of India.[14]

We first identified the parameters of analysis based on whether these parameters are legally recognised in contemporary data protection legislation and mandated to be disclosed in the privacy policies/ notice for informed consent for data processing. Internationally, our reference points included the United States' Health Insurance Portability and Accountability Act 1996 (HIPAA) and the Standards for Privacy of Individually Identifiable Health Information 2000 (HIPAA Privacy Rule); the European Union's General Data Protection

[11] United Nations General Assembly, *Universal Declaration of Human Rights* (United Nations, 1948), art. 12; United Nations General Assembly, *International Covenant on Civil and Political Rights* (United Nations, 1966), art. 17.
[12] United Nations General Assembly, International Covenant on Economic, Social and cultural Rights (United Nations, 1966), art. 12.
[13] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 14: The Right to the Highest Attainable Standard of Health (Article 12 of the International Covenant on Economic, Social and Cultural Rights)*, UN Doc. E/C.12/2000/4 (11 August 2000).
[14] *Justice K.S. Puttaswamy (Retd) vs Union of India*, *2019 (1) SCC 1*.

Regulation 2016 (GDPR); Brazil's Lei Geral de Proteção de Dados Pessoais 2018 (LGPD); Thailand's Personal Data Protection Act 2019 (PDPA); and the Nigerian Data Protection Act 2023 (NDPA). Domestically, we drew on the DPDPA 2023. Table 1 provides the list of parameters, with their legal and disclosure status under the cited legal frameworks. Finally, we organised the parameters of analysis into four categories: notice and consent, privacy principles, user rights, and transparency and accountability.

Table 1: Comparative legal analysis of identified parameters - whether recognised and mandated to be disclosed in privacy policy/notice for consent

Parameter	HIPAA United States	GDPR European Union	LGPD Brazil	PDPA Thailand	NDPA Nigeria	DPDPA India
Notice and consent						
Requirement of notice/ consent	Recognised (S. 164.520)	Recognised (Art. 12, 13, 14)	Recognised (Art. 8, 9, 18)	Recognised (S. 19, 23(1))	Recognised (S. 27(1), 27(3))	Recognised (S. 5, 6)
Nature of consent	Recognised Informed and Express consent (S.164.520(b))	Recognised Informed and Express consent (Art. 7)	Recognised Informed and Express consent (Art. 8)	Recognised Informed and Express consent (S.19)	Recognised Informed and Express consent (S.26(7))	Recognised Informed and Express consent (S. 6(1))
Timing of notice/ consent	Recognised Enrolling in a health plan or first service delivery S.164.520(c)	Recognised At the time of collecting personal data Art. 13(1))	Recognised Before or during processing (Art. 7(1), 7(v), 9(1), 18))	Recognised Before or during processing (S. 19)	Recognised Before processing (S. 27(1))	Recognised Before or during processing (S. 5)
Multilingual access	Not recognised	Not recognised	Not recognised	Not recognised	Not recognised	Recognised (S. 6(3))
Information on categories of data collected	Recognised express disclosure mandate (S. 164.508(c)(1)(i) 164.520(b)(1)(ii))	Recognised express disclosure mandate (Art. 14(1)(d))	Recognised, implied disclosure mandate (Art. 9, 18)	Recognised express disclosure mandate (S. 23(3))	Recognised implied disclosure mandate (Ss. 24, 27, 34(1)(a)(ii))	Recognised express disclosure mandate (Ss. 5(1)(i), 5(2)(a)(i))
Information on third-party recipients of data	Recognised express disclosure mandate (S. 164.508, 164.520(b)(1)(ii)(H))	Recognised express disclosure mandate (Art. 13(1)(e))	Recognised express disclosure mandate (Art. 9(VIII), 18(VII))	Recognised express disclosure mandate (S. 23(4))	Recognised express disclosure mandate (S. 27(1)(c))	Recognised as a right to seek information. But no disclosure mandate in notice (S. 11(1))
Right to withdraw consent	Recognised express	Recognised express	Recognised express	Recognised express	Recognised express	Recognised express

Table 1: Comparative legal analysis of identified parameters - whether recognised and mandated to be disclosed in privacy policy/notice for consent						
Parameter	**HIPAA United States**	**GDPR European Union**	**LGPD Brazil**	**PDPA Thailand**	**NDPA Nigeria**	**DPDPA India**
	disclosure mandate S. 164.508, 164.520(b)(1)(ii)(E)	disclosure mandate (Art. 13(2)(c))	disclosure mandate (Art. 8(5))	disclosure mandate (S. 23(6), 33(2))	disclosure mandate (Ss. 26(4), 27(1)(d), 35(1))	disclosure mandate (Ss. 5(1)(ii), 6(4))
Privacy principles						
Lawfulness and fairness in processing data	Recognised implied disclosure mandate (S. 164.502(a), 164.520(b)(1)(ii))	Recognised express disclosure mandate (Art. 13(1)(c), 5(1)(a))	Recognised express disclosure mandate (Art. 6, 7)	Recognised express disclosure mandate (S. 3)	Recognised express disclosure mandate (S. 24(1)(a), 27(1)(b))	Recognised as a legal basis but no specific disclosure mandate (S. 4)
Purpose(s) of processing	Recognised express disclosure mandate (S. 164.502(a), 164.508(a), 164.520(b)(1)(ii))	Recognised express disclosure mandate (Art. 13(1)(c), 5(1)(b))	Recognised express disclosure mandate (Art. 6(1), 9(1))	Recognised express disclosure mandate (S. 23(1))	Recognised express disclosure mandate (Ss. 27(1)(b), 24(1)(b))	Recognised express disclosure mandate (S. 5(1)(i), 6(1))
Data minimisation	Recognised no disclosure mandate (S.164.502(b))	Recognised no disclosure mandate (Art. 5(1)(c))	Recognised no disclosure mandate (Art. 6(3))	Recognised no disclosure mandate (S. 22)	Recognised no disclosure mandate (S. 24(1)(c))	Recognised no disclosure mandate (S. 6(1))
Storage limitation	Not recognised	Recognised express disclosure mandate (Art. 13(2)(a), 5(1)(e))	Recognised express disclosure mandate (Art. 15, 16)	Recognised express disclosure mandate (S. 23(3))	Recognised express disclosure mandate (Ss. 27(1)(e), 24(1)(d))	Recognised as obligation of data fiduciary but no disclosure mandate in notice (S. 8(7))
Accuracy	Recognised implied disclosure mandate (S. 164.526, 164.520(b)(1)(iv)(D))	Recognised no disclosure mandate (S. 5(1)(d), 18(1)(a))	Recognised no disclosure mandate (Art. 6(v))	Recognised no disclosure mandate (S. 35)	Recognised no disclosure mandate (Ss. 24(1)(e), 24(1)(f))	Recognised no disclosure mandate (Ss. 8(3), 12)
Data security	Recognised express	Recognised disclosure mandate	Recognised disclosure mandate	Recognised disclosure mandate	Recognised disclosure mandate	Recognised no disclosure mandate

Table 1: Comparative legal analysis of identified parameters - whether recognised and mandated to be disclosed in privacy policy/notice for consent						
Parameter	**HIPAA United States**	**GDPR European Union**	**LGPD Brazil**	**PDPA Thailand**	**NDPA Nigeria**	**DPDPA India**
	disclosure mandate (S. 164.302-18, 164.520(b)(1)(v)(A))	(A. 32)	(Art. 6(x), 46)	(S.37)	(Ss. 24(1)(f), 24(2), 44)	(Ss. 8(4), 8(5))
User rights						
Access information about personal data	Recognised, express disclosure mandate (S. 164.524, 164.520(b)(1)(iv)(B), (C) & (E))	Recognised, express disclosure mandate (Art. 13(2)(b) Art. 15)	Recognised, express disclosure mandate (Art. 18(I))	Recognised, express disclosure mandate (Ss. 23(6), 30(1), 39(5))	Recognised, express disclosure mandate (Ss. 27(1)(d), 34(1)(a)(v))	Recognised, no disclosure mandate (S.11(1))
Erasure of personal data	Not recognised	Recognised, express disclosure mandate (Art. 13(2)(b), 17)	Recognised, express disclosure mandate (Art. 18(VI))	Recognised, express disclosure mandate (Ss. 23(6), 33)	Recognised, express disclosure mandate (Ss. 27(1)(d), 34(1)(a)(v), 34(1)(d))	Not recognised
Rectification of personal data	Recognised, express disclosure mandate (S. 164.526, 164.520(b)(1)(iv)(D))	Recognised, express disclosure mandate (Art. 13(2)(b), 16)	Recognised, express disclosure mandate (Art. 18(III))	Recognised, express disclosure mandate (Ss. 23(6), 33)	Recognised, express disclosure mandate (Ss. 27(1)(d), 34(1)(a)(v), 34(1)(c))	Recognised, no disclosure mandate (S. 12)
Request information about automated decision-making	Not recognised	Recognised, express disclosure mandate (Art. 13(2)(b), 13(2)(f), 22)	Recognised, express disclosure mandate (Art. 20)	Recognised, express disclosure mandate (S. 31)	Recognised, express disclosure mandate (Ss. 27(1)(g), 34(1)(a)(viii))	Not recognised
Seek explanation and object to automated decision-making	Not recognised	Recognised, express disclosure mandate (Art. 13(2)(f), 22)	Recognised, express disclosure mandate (Art. 20)	Recognised, express disclosure mandate (S. 31)	Recognised, express disclosure mandate (S. 27(1)(g))	Not recognised
Object to processing of personal data,	Recognised, express	Recognised, express	Recognised, express	Recognised, express	Recognised, express	Not recognised

Table 1: Comparative legal analysis of identified parameters - whether recognised and mandated to be disclosed in privacy policy/notice for consent						
Parameter	**HIPAA United States**	**GDPR European Union**	**LGPD Brazil**	**PDPA Thailand**	**NDPA Nigeria**	**DPDPA India**
inc. direct marketing	disclosure mandate (Ss. 164.510, 164.520(b)(1)(iv)(A))	disclosure mandate (Art. 13(2)(b), 21)	disclosure mandate (Art. 18(2))	disclosure mandate (S. 32)	disclosure mandate Ss. 27(1)(d), 27(1)(g), 34(1)(a)(v), 36(1)(4))	
Data portability	Recognised, express disclosure mandate (S. 164.524, 164.520(b)(1)(iv)(C))	Recognised, express disclosure mandate (Art. 13(2)(b), 20)	Recognised, express disclosure mandate (S. 18(V), 19(3))	Recognised, express disclosure mandate (S.30)	Recognised, express disclosure mandate (Ss. 27(1)(d) 34(1)(b))	Not recognised
Right to nominate	Not recognised	Not recognised	Not recognised	Not recognised	Not recognised	Recognised, no disclosure mandate. S. 14
Transparency and Accountability						
Information on cross border flow of data	Not recognised	Recognised, express disclosure mandate (Art. 13(1)(f))	Recognised, express disclosure mandate (Art. 9(VII), 33(VII))	Recognised, express disclosure mandate (Ss. 23(4), 28(2))	Recognised, express disclosure mandate (Ss. 27(1)(c), 34(1)(a)(iii), 43(1)(a))	Recognised, no disclosure mandate (Ss. 11, 16)
Contact details of DPO/GRO	Recognised, express disclosure mandated (S. 164.530(a)(1), 164.520(b)(1)(vi))	Recognised, express disclosure mandate (Art. 13(1)(b), 13(2)(d))	Recognised, express disclosure mandate (Art. 41(1))	Recognised, express disclosure mandate (S. 23(5))	Recognised, express disclosure mandate (S. 27(1)(a))	Recognised, express disclosure mandate (Ss. 6(3), 8(9))
Grievance redress process	Recognised, express disclosure mandate (S. 164. 530(d), 164.20(b)(1)(vi))	Recognised, express disclosure mandate (Art. 13(2)(d))	Recognised, express disclosure mandate (Art. 18(1))	Recognised, express disclosure mandate (S. 73)	Recognised, express disclosure mandate (S. 27(1)(f))	Recognised, express disclosure mandate (Ss. 5(1)(ii), 5(2)(a)(ii), 8(10), 13)
Information on updates or alterations to notice or consent terms	Recognised, express disclosure mandate S. 164.530(i)(4) 164.520(b)(3)	Recognised, express disclosure mandate (Art. 13(3))	Recognised, express disclosure mandate (Art. 8(6), 9(2))	Recognised, express disclosure mandate (S. 23)	Not recognised	Not recognised

Table 1: Comparative legal analysis of identified parameters - whether recognised and mandated to be disclosed in privacy policy/notice for consent						
Parameter	**HIPAA United States**	**GDPR European Union**	**LGPD Brazil**	**PDPA Thailand**	**NDPA Nigeria**	**DPDPA India**
Date breach notification	Recognised, no disclosure mandate (S.164.404)	Recognised, express disclosure mandate (Art. 34)	Recognised, express disclosure mandate (Art. 48)	Recognised, express disclosure mandate (S. 37.5)	Recognised, express disclosure mandate (S. 2.6(c))	Recognised, no disclosure mandate (S. 8(6))

We supplemented the legal analysis with a technical examination of the user journey on the selected telemedicine web platforms. Specifically, we examined the availability and visibility of privacy policy, the timing of the privacy and/or consent notice, the nature of consent, and disclosure of third party data-sharing practices. The legal and technical analyses were conducted from October 2024 to August 2025.

For the first three parameters, we manually browsed the websites and attempted to register on the selected platforms to note the presence and placement of privacy policies, consent mechanisms such as data collection banners, the timing of consent requests, and whether consenting entailed affirmative action by the user.

For the fourth parameter, we conducted network activity analysis using the HTTP Toolkit, an open-source network debugging and interception tool that enables inspection of HTTP requests and responses, and identification of data flows to third-party services.[15] The HTTP Toolkit has been used in prior digital privacy research.[16] In the first step, we configured the Toolkit to launch and control a new Chrome browser session, which allowed us to capture all network requests in real time throughout the user journey. The payloads of these requests were inspected and decoded using the Toolkit's built-in tools. In select cases, we used GitHub Copilot to help interpret obfuscated variable names or complex code, translating it into clear, human-readable explanations. From the comprehensive set of captured requests, we extracted and reported the HTTPS requests that contained either health-related information or personally identifiable information. This selective focus ensured that our findings centered on data transmissions with potential privacy or security implications, providing a targeted view of the most significant risks. Finally, we tracked the user journey across three service pathways: teleconsultations, medicine purchase, and lab booking. Beginning with the landing page, we noted any third-party calls made immediately upon page load. We then observed the process of service search or selection, such as choosing a doctor, medicine or lab test, followed by patient or order selection, and finally the scheduling and checkout process. To

[15] Saikishore K, *HTTP Toolkit: Your Gateway to Effortless Network Analysis*, CaratLane Insider (12 December 2024) https://inside.caratlane.com/http-toolkit-your-gateway-to-effortless-network-analysis-5d7076176e66

[16] Christopher Boyd, *"Exposing the Hidden Data Ecosystem of the UK's Most Trusted Charities"*, ProPrivacy (10 September 2020) https://proprivacy.com/privacy-news/exposing-the-hidden-data-ecosystem-of-the-uks-most-trusted-charities

avoid completing actual transactions, we terminated the journey just before a payment or confirmation was required.

The limitations of our technical analysis include its focus on frontend tracking and the potential inaccuracy of variable interpretation. We restricted our analysis to the frontend because accessing backend requests is not feasible within the scope of this work. Backend traffic is typically encrypted (e.g. HTTPS), and decryption would require access to server-side keys or the use of interception techniques that are neither legally nor ethically permissible. In addition, we occasionally relied on GitHub Copilot to assist in interpreting complex JavaScript code for our own understanding. This introduces the possibility that some variables may have been interpreted differently from their intended meaning. Where such interpretations occur, we present them as possibilities rather than definitive findings.

Table 2 presents the broad categories of analysis, the accompanying description, the parameters classified within each category and the methodological approach applied to each parameter.

Table 2: Framework of analysis

Category	Description	Parameters	Type of analysis
Notice and consent	International human rights law recognises the salience of individual autonomy for the protection of the right to privacy. According to General Comment No. 16, every individual should be able to ascertain, in an intelligible form, what personal data is stored in automatic files, for what purposes and which public or private entities may control their files.[17] The principle is also reflected in international and domestic laws cited by us.	Availability and visibility of privacy policy	Technical
		The timing of privacy policy	Technical
		Nature of consent	Legal and technical
		Multilingual access	Legal
		Disclosure of purposes, data collected and third-party recipients	Legal and technical
		Right to withdraw consent	Legal
Privacy principles	The right to privacy is anchored in a set of principles that facilitate proper processing of personal data, i.e. lawfulness and fairness in processing,	Purpose limitation	Legal
		Data minimisation	Legal
		Storage limitation	Legal

[17] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

Table 2: Framework of analysis			
Category	**Description**	**Parameters**	**Type of analysis**
	purpose limitation, data minimisation, storage limitation, accuracy and data security.[18] These principles are also affirmed by the legal instruments referenced in our analysis.	Accuracy	Legal
		Data security	Legal
User rights	International and domestic legislations affirm a set of rights that empower individuals to exercise meaningful control over their personal data. These include the rights to access information, erasure, rectification, request information about automated decision-making, seek explanation and object to automated decision-making, object to processing of personal data including direct marketing, and data portability. The DPDPA is the only legislation which recognises the right to nominate an authorised representative.	Access information about personal data	Legal
		Erasure of personal data	Legal
		Rectification of personal data	Legal
		Request information about automated decision-making	Legal
		Seek explanation and object to automated decision-making	Legal
		Object to processing of personal data, inc. direct marketing	Legal
		Data portability	Legal
		Right to nominate	Legal
Transparency and accountability[19]	The human right to privacy requires that data controllers must process personal data transparently.[20]Transparency demands individuals must be informed about the processing conditions to which their personal data will be subject at the time of collection.	Information on cross border flow of data	Legal
		Contact details of DPO	Legal
		Contact details of GRO	Legal
		Grievance redress process	Legal
		Information on updates or alterations to notice or	Legal

[18] UN Special Rapporteur on the Right to Privacy, *A/77/196: Principles Underpinning Privacy and the Protection of Personal Data*, 20 July 2022.
[19] While several parameters listed earlier promote transparency, here we focus on aspects that have not yet been included.
[20] UN Special Rapporteur on the Right to Privacy, *A/77/196: Principles Underpinning Privacy and the Protection of Personal Data*, 20 July 2022.

Table 2: Framework of analysis			
Category	**Description**	**Parameters**	**Type of analysis**
	Additionally, data controllers should communicate the channels available to individuals for accessing information and seek redress regarding the handling of their data.	consent terms	
		Data breach notifications	Legal

5 Findings

5.1. Notice and consent

5.1.1 Availability and visibility of the privacy policy

All eight commercial web platforms had displayed privacy policies on their webpages. However, they were placed in the footer of the webpage. eSanjeevani's webpage did not have a standalone privacy policy. Its privacy policy was placed inside a document titled 'Website Policy' in the 'Standards and Guidelines' section of its webpage. PharmEasy, Netmeds, Tata 1mg, MediBuddy and Apollo 24/7 linked their privacy policies to login/registration. However, data collection begins even before logging in or registering. On analysis of whether the placement of the privacy policies met the standards of informed consent, we find that while all nine web platforms technically complied with displaying a privacy policy, their placement, mostly buried in webpage footers or embedded in broader documents, as in the case of eSanjeevani, raises concerns about accessibility and visibility. For users, especially those with limited digital literacy, such placement can make it difficult to locate, understand, and exercise their data rights, thereby undermining transparency and informed consent.

5.1.2 Timing of serving the privacy policy and taking consent

Many platforms failed to explicitly present their privacy policies or direct users to them at the time of data collection (e.g. browsing, during login or registration). Web platforms such as MedPlusMart, Lybrate and eSanjeevani did not mention or display the privacy policies during user navigation at the time of registration/login. PharmEasy, Netmeds, Tata 1mg, MediBuddy, Apollo 24/7 linked their privacy policies at the time of login/registration, but provided no mechanism to collect users' consent by an affirmative action (for eg. by providing a checkbox). Practo provides the link to 'terms' at the time of registration, which further contains a link to the privacy policy. The user can access the privacy policy only upon clicking the link to 'terms'.

On analysis, we found that the web platforms were failing to obtain informed consent before or at the time of data collection. In many cases, users were either not directed to the privacy policy at the point of data collection (e.g., during login or registration) or were only provided

a passive link without any mechanism for affirmative consent, such as a checkbox. Importantly, data collection does not begin only at registration or login. it starts the moment users browse the website or app (through cookies, trackers, or log data). The absence of clear notice and explicit consent at this earlier stage further undermines user awareness and weakens the requirements of transparency, accountability, and informed consent

5.1.3 Nature of consent

Explicit, unambiguous and affirmative consent

Consent to data processing is implied in the privacy policies across all nine web platforms. The privacy policies stated that signing up, browsing, using app services, and voluntarily sharing personal information, will amount to consenting to the terms of the privacy policy.

The technical analysis showed that none of the nine web platforms facilitated unambiguous, explicit consent necessitated by an affirmative action on the part of the users. eSanjeevani, MedPlusMart and Lybrate did not mention consent at any time in the user journey. Apollo 24/7, PharmEasy, MediBuddy, Tata 1mg, Netmeds and Practo stated that consent was implied by continuing to login/register – *"by logging in/registering, you agree to the terms of the privacy policy or terms of use.*" None of the web platforms had any checkbox requiring users to affirmatively give their consent. Practo provided a checkbox only for the purpose of consenting to email and marketing communication, but that was also pre-ticked and did not support explicit opt-in consent.

Without a requirement for users to actively by an affirmative action accept the privacy policy (e.g., via an unchecked checkbox), these web platforms do not meet best practice or legal standards for valid informed consent under modern data protection laws.

Granular consent

None of the nine web platforms facilitated granular, and unbundled consent to the clauses of the privacy policy. All the policies were "take it or leave it." Some web platforms mentioned taking specific consent only for some technical permissions. For instance, MediBuddy takes express consent to access the location, camera or photo gallery.

The technical analysis of the web platforms also revealed that granular consent is limited to technical permissions for location (Lybrate, Apollo24/7, Practo, Netmeds, Tata 1mg) and notifications (MedPlusMart, Lybrate, PharmEasy) only. If the user agrees to share her location on the application, it automatically identifies the user, using the latitude and longitude coordinates on the user's device. In cases where permission is not given, the default location present in the web application is still used. In both cases, the location information is collected and shared with third parties in Practo, Lybrate and MedPlusMart. This implies that the user has no real choice to opt out of location sharing. Such location sharing practices raise concerns over privacy, transparency and consent.

The findings of the legal as well as technical analysis reveal that none of the nine web platforms provide granular and unbundled consent to users regarding categories of data

collected and the purposes for processing and sharing, which undermines specific, meaningful consent and autonomy.

5.1.4 Multilingual access

The privacy policies of the selected telemedicine web platforms are available exclusively in English, with no options for multilingual access provided by any of the platforms. This significantly limits accessibility for large sections of India's population, undermining the principles of transparency and informed consent.

5.1.5 Disclosures on categories of data collected

An analysis of the privacy policies of the nine web platforms reveals the collection of a wide range of data points. Table 3 categorises the types of data collected into five groups: contact and demographic; physical, physiological and mental health status and medical histories; financial and payment details; usage, browser and device details; and miscellaneous data. The common data points across all web platforms include name, data of birth or age, email address, phone number, physical address, gender, and medical records and history. All commercial web platforms, collect detailed device and financial information. On average, each platform collects about 30 distinct data points. Tata 1mg leads with the most extensive data collection practices, capturing 41 unique data points, followed by Practo with 34 unique data points. Notably, Tata 1mg collects the largest volume of data across all data categories, and is the only platform that gathers sensitive demographic attributes including marital status, occupation, ethnicity and religion. In terms of health-specific data, Tata 1mg again ranks highest with nine distinct health-related entries, while Lybrate and Apollo 24/7 follow closely with eight each. By contrast, eSanjeevani collects the least amount of data with just twelve distinct data points identified.

Our technical analysis reveals that all commercial platforms collect usage and device data via first party as well as third party cookies/trackers.[21] However, legal analysis reveals that Apollo 24/7 does not categorically state whether it uses third party cookies in their privacy policies. Futher, MediBuddy mentions the use of first party cookies only. Importantly, none of the web platforms display a cookie consent banner, except Netmeds. it is important to note that the web platforms may not explicitly list every specific data point collected under the term 'usage data'. The term usage data, typically refers to a broad range of information about how users interact with the platform, the technical environment they use (device/network information), and patterns of their behaviour (behavioural data). These data points are collected to help the platform understand user engagement, improve functionality and aid in security; and also for personalisation, analytics and targeted advertisement. If a platform uses third party trackers, they often collect additional behavioural and device metadata, which can

[21] First-party cookies are created and stored directly by the website a user visits. They are primarily used to remember user preferences, login details, and site analytics within that domain. Third-party cookies are created by domains other than the one a user is visiting. They are often embedded through advertising pixels, analytics scripts, or social media plugins, allowing tracking of users across multiple websites for profiling and targeted advertising. *Information Commissioner's Office (ICO)*, *Cookies and Similar Technologies* (UK ICO, 2023) https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

be part of the broader usage data ecosystem.[22] Collection of usage data and third-party tracker data implies some level of user profiling for analytics and personalisation, which carries implications for user privacy and requires explicit consent.

We also analysed the data points collected to assess the risk of device fingerprinting across web platforms. Device fingerprinting is a method of tracking and identifying users online by collecting a unique combination of information about their device, browser, and system settings, without relying on cookies.[23] Together, these create a "digital fingerprint" that can uniquely identify a user's device when they visit websites or apps, even if cookies are deleted or private browsing is used.[24] This practice raises privacy concerns because it is often invisible to users and difficult to opt out of, effectively bypassing consent mechanisms like cookie banners. PharmEasy and MediBuddy collect the most comprehensive set of usage and device data. In fact, PharmEasy and Lybrate explicitly mention collections of a "unique device identifier" and "device identifiers" respectively. Though the privacy policies do not list down the specific types of device identifiers collected, in practice they usually include identifiers tied to a user's specific device, such as an IMEI number, advertising ID, or another hardware-based identifier that can be used to uniquely identify and track a device consistently across sessions.[25] Collecting unique device identifiers, alongside other data like IP address, operating system, browser type/version, user agent, and location, signifies that PharmEasy and Lybrate, gather comprehensive device and usage metadata that especially in combination with embedded third-party trackers, could enable robust device fingerprinting and persistent user identification across platforms. In fact all the commercial web platforms collect significant "usage data" and varying amounts of browser, network and device information, which can be combined to create a unique fingerprint that can track the users device across different apps or websites. In February 2025, Google officially allowed advertisers and sites using its technology, to use digital fingerprinting to create persistent device profiles for cross-site identification, even if users clear cookies or block trackers.[26] Our technical analysis confirms the presence of third-party trackers from Google Analytics, Microsoft and Meta on all the commercial platforms, and that a wide range of data points are shared with them, which significantly increases the likelihood of the commercial web platforms engaging in device fingerprinting.

---

[22] Stephen Hateley, *"What Is Usage Data and How Do Businesses Use It?"*, DigitalRoute Blog (26 September 2024) https://www.digitalroute.com/blog/usage-data/

[23] European Data Protection Board (EDPB) *Guidelines 05/2020 on Consent under Regulation 2016/679 (GDPR)*: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[24] Peter Eckersley, *How Unique Is Your Web Browser?* (PETS 2010): https://coveryourtracks.eff.org/static/browser-uniqueness.pdf

[25] Rich Keith, *"What Is Device ID? Significance and Applications"*, Ping Identity Blog (3 January 2025) https://www.pingidentity.com/en/resources/blog/post/device-id.html

[26] Pieter Arntz, *"Google now allows digital fingerprinting of its users"*, Malwarebytes Blog (19 February 2025) https://www.malwarebytes.com/blog/news/2025/02/google-now-allows-digital-fingerprinting-of-its-users

Table 3: Summary of findings on the categories of data collected as stated in the privacy policies					
Website	**Contact and demographic data**	**Health data**	**Financial data**	**Device, Network & Browsing data**	**Miscellaneous data**
Tata 1mg	Name, DOB, email, address, phone, gender, nationality, marital status, ID card, occupation, marital status, ethnicity, religion	Medical history and records, health status, treatment plans and medication, dosage details, alternative medication, medicines ordered from Tata 1mg, lab tests, other info	Payment instrument information, transactions, transaction history, preferences, method, mode and manner of payment, spending pattern or trends	Usage data, browser type/version, referring URLs, log files, IP address, browser type/version, OS	Product/service use data, loyalty programme info, reviews, feedback, app permissions for location, camera, photo/media/ files, sms, wifi, record audio, bluetooth, employer, travel history First & third party cookies
Lybrate	Name, DOB, email, address, gender	Physical, physiological and mental health conditions, sexual orientation, medical records & history, login ID, password, location	Bank account, credit card, debit card, other payment instrument details	Usage data, pattern of use, features used, the amount of storage used, transaction data, log files, IP address, browser type/language, referring URL, OS, network details eg. ISP name/network type, diagnostic data, device identifiers (from app).	Camera, microphone, contact book, First and third party cookies
Apollo 24/7	Name, DOB, address, email, phone, gender, nationality	Physical, physiological and mental health conditions, medical records & history, insurance coverage, prescription, search & appointment history, lab data, radiology data, epharmacy order data.	Bank account, credit card, debit card, PAN	Usage data, log files, browsing and search history, URL of referral site, browser type/version, ISP name, IP address, OS,	Mention cookies. But does not specify whether it uses first and/or third party cookies

Table 3: Summary of findings on the categories of data collected as stated in the privacy policies					
Website	**Contact and demographic data**	**Health data**	**Financial data**	**Device, Network & Browsing data**	**Miscellaneous data**
Practo	DOB, email, phone, pincode, country, gender, User ID, password	passwords, biometric data, health records, images/documents/files, treatment availed, health conditions, sexual orientation, Insurance info,	bank accounts, credit and debit card details or other payment instrument ls	Usage data, referral URL, IP address, browser type/version, OS, email pattern, ISP name, cookies	feedback data, call data records, visitor details at registration, First and third party cookies
Netmeds	Name, DOB, email, address, mailing address, phone number, contact preferences, gender	Physical, physiological and mental conditions, medical records, Usage and interaction data, biometric information, password,	Bank account, credit card, debit card, other payment instrument	Usage data, referring URL, exit URL, navigation patterns, log files, IP address, browser type/version, OS, email pattern, ISP name, internal domain & host names	First and third-party cookies
PharmEasy	Name, phone number, email and residential address	Health information and status, health & medical history, Medical records, treatment notes, items placed in the cart, purchased, lab reports, prescriptions, dosage details	Credit/card number, other payment details, expiration date,	internet domain and host names, IP addresses, browser software, OS, stream patterns, and dates and times of accessing site. OS type and version, App version, device brand, browser and its version details, User agent, location including a unique device identifier	Data from advertisers, partners, third parties First and third-party cookies

Table 3: Summary of findings on the categories of data collected as stated in the privacy policies					
Website	**Contact and demographic data**	**Health data**	**Financial data**	**Device, Network & Browsing data**	**Miscellaneous data**
MediBuddy	Name, DOB, address, email, phone, employee code, ID card, family members / dependent information	Physical, physiological and mental health conditions, medical records & history, family member/dependent data	Bank account, other payment instrument detail	Usage data, browser type/version, browsing information (pages visited, navigation patterns), log files, IP address, OS, ISP name/network type & connection logs,	Location, camera, photo gallery, files/folders, Apple HealthKit metrics (steps, weight, BP, etc.), Aggregated health info, usage data Mentions first party cookies only
MedPlusMart	Name, DOB, email, address, residential address, phone/mobile no. gender.	Physical, physiological and mental health conditions, medical records & history, family member data, blood group,	Bank account, other payment instrument detail expiration date and/or other payment instrument details and tracking information from cheques or money orders.	date and time of accessing services; referral URL; browser details, search engine, search terms & advertising clicks/actions; survey's response; manufacture & model of mobile device; mobile OS; mobile internet browser; geo-location; session logs; IP address, ISP name; OS; Information required for personalisation	Location, camera, photo gallery, files/folders, Apple HealthKit metrics (steps, weight, BP, etc., information about buying behaviour, personal correspondence, messages posted on message boards, chatrooms first and third-party cookies
eSanjeevani	Name, DOB, email, address, phone, gender	Health records, dependent info, patient ID	Not specified	Not specified	No cookies mentioned

5.1.6 Disclosure of purposes for data collection and processing

We analysed the purposes stated by the platforms for the collection and processing of personal data and categorised them as:

a) *Primary and core purposes of service delivery* - all the platforms process personal data for core service delivery, including, user registration and authentication, grievance redress and customer support (eSanjeevani does not explicitly mention customer support), and for maintaining health records and medical history. Other core functions include enabling consultation with healthcare providers - Apollo 24/7, Practo, Lybrate, Tata 1mg, and booking lab tests - Netmeds, Tata 1mg, PharmEasy, Practo, Apollo 24/7, MediBuddy, MedPlusMart. E-pharmacies - Netmeds, Tata 1mg, MedPlusMart, PharmEasy do not provide doctors consultations, but collect health data while processing prescriptions or orders.

b) *Operational and technical functions* - This category of purposes includes payment, platform security and fraud detection, system diagnostics and troubleshooting, data analytics and service improvement (all platforms, except eSanjeevani).

c) *Marketing and profiling* - All platforms, except eSanjeevani, process personal data for analytics and for marketing purposes, such as targeted advertisement and personalised recommendations (Lybrate references promotions but is less explicit); behavioural advertising and internet-based tracking (PharmEasy, Practo, Apollo 24/7, Netmeds, Tata 1mg, MediBuddy, MedPlusMart - inferred for some as their policies mention cookies/SDKs); retargeting and remarketing campaigns (Apollo 24/7, Netmeds, PharmEasy - implied via SDK use - but poorly disclosed). eSanjeevani is the only platform that clearly excludes commercial profiling/targeting.

d) *Research* - Tata 1mg, Practo, Netmeds, Apollo 24/7, PharmEasy explicitly state that they carry out internal research for trend analysis and market improvement. Only eSanjeevani states that they use anonymised data for public health research purposes.

Next, we analysed whether the disclosure of purposes was adequate for enabling meaningful, informed and specific user consent. We found that the disclosures do not support informed, specific and unambiguous user consent, for the following reasons: *first,* we found that most platforms (MediBuddy, MedplusMart, Apollo 24/7, NetMeds, Practo, Tata 1mg) list some vague and overbroad purposes - *"business purposes", "product improvement", "as we deem necessary."* These generic phrases are used without the necessary specificity and fail to clarify the specific nature or scope of processing, which undermines informed consent. Further, we found use of catch-all future expansion phrases – *"as required", "such other purposes", "any business purposes"* that enable unspecified future use without taking fresh consent. Embedding vague and catch-all clauses allow commercial platforms to collect personal data for indefinite future use without user control. *Second,* none of the platforms categorise purposes into core/primary purposes and other purposes. Core purposes are

bundled with other purposes, such as analytics, commercial research, marketing and advertising purposes. *Third,* None of the platforms facilitate granular user consent on the basis of core and other purposes. Fourth, use of anonymised/aggregated data for research or business intelligence is mentioned but not adequately explained or accompanied by user choice. Fifth, some platforms use analytics to build algorithms, scoring systems and recommendation engines (explicitly mentioned by Tata 1mg, Practo, Apollo 24/7, MediBuddy, MedPlusMart, PharmEasy). This implies use of AI/ML systems, but these platforms do not specifically disclose that they use AI/ML and have no mention of corresponding rights of users when AI/ML systems are used in a way that would have an impact on them.

5.1.7 Disclosures on third-party recipients of data

Table 4 - Legal analysis – Third-Party Data Sharing Practices of Indian Telemedicine Platforms

Platform	Recipient Categories	Purposes Disclosed	Ad / Analytics Integrations	Third-Party Cookie / Tracker	Opt-Out / Consent Controls	Unique / Concerning Practices
Tata 1mg	Affiliates, partners, group entities, service providers, law enforcement, business transfers	Service delivery, payments, analytics, ads, promotions, research, compliance; cross-border transfers	Targeted ads, remarketing, SDK integrations, session replay	Mentions third party cookies	No granular consent; no cookie banner; opt-out from personalised marketing not clearly stated	Loyalty/reward programme sharing of purchase and behavioural data with external partners
Lybrate	Service providers, affiliates, partners, legal authorities	Service delivery, payments, analytics, ads, promotions, research (no cross-border transfer stated)	Analytics & ads (via trackers and cookies)	Mentions third-party cookies	Opt-out from personalised marketing allowed	—
Apollo 24/7	Affiliates, service providers, partners, legal authorities	Service delivery, payments, analytics, ads, research, compliance; cross-border transfers stated	Remarketing via partners, ad targeting	Does not specifically mention third party cookies (but found in analysis)	No granular consent; no opt-out for ads	—

Table 4 - Legal analysis – Third-Party Data Sharing Practices of Indian Telemedicine Platforms						
Platform	**Recipient Categories**	**Purposes Disclosed**	**Ad / Analytics Integrations**	**Third-Party Cookie / Tracker**	**Opt-Out / Consent Controls**	**Unique / Concerning Practices**
Practo	Affiliates, partners, service providers, legal authorities	Service delivery, payments, analytics, ads, promotions, research, compliance, cross-border transfers	Targeted ads, session replay analytics, remarketing	Mentions third-party cookies	Opt-out from personalised marketing allowed. No cookie consent banner.	Sale of de-identified / aggregated data mentions DND override without separate consent
Netmeds	Affiliates, group companies, service providers, partners, legal authorities	Service delivery, payments, analytics, ads, promotions, research, cross-border transfers	Remarketing, targeted ads	Mentions third-party cookies	Cookie consent banner (only platform with one)	—
PharmEasy	Affiliates, group companies, partners, service providers, legal authorities	Service delivery, payments, analytics, ads, promotions, research, cross-border transfers	Targeted ads, SDK integrations, session replay analytics	Mentions third-party cookies	No granular consent No cookie consent banner	Sale of de-identified / aggregated data
MediBuddy	Service providers, partners, affiliates, legal authorities, employers (in corporate plans)	Service delivery, payments, analytics, ads, promotions, research. No cross-border transfer stated	Analytics & ads (via embedded trackers)	Mentions first party cookies only (third party trackers found in analysis)	No granular consent No cookie consent banner	Shares personal data with employers; reserves right to transfer data “in sole discretion”
MedPlusMart	Affiliates, partners, service providers, legal authorities	Service delivery, payments, analytics, ads, promotions, research. No cross-border transfer stated	Analytics & ads (via trackers and cookies)	Mentions third-party cookies	Opt-out from personalised marketing allowed No cookie consent banner	Affiliates/partners can use shared data for marketing unless user opts out (process unclear)

Table 4 - Legal analysis – Third-Party Data Sharing Practices of Indian Telemedicine Platforms						
Platform	**Recipient Categories**	**Purposes Disclosed**	**Ad / Analytics Integrations**	**Third-Party Cookie / Tracker**	**Opt-Out / Consent Controls**	**Unique / Concerning Practices**
e-Sanjeevani	Govt. agencies, researchers (public health only), service providers for infrastructure	Core service delivery, non-commercial analytics, public health research, compliance.No cross-border transfer stated	No advertising or commercial analytics integrations	No mention of third-party cookies No third-party cookies found	Not applicable for ads; no commercial sharing	Data to be shared with "persons carrying out the intended medical and administrative interventions"

An analysis on the scope of data sharing among the platforms examined, shows that personal data is shared with third-parties for the purposes of: core service delivery (all platforms); payment processing (all platforms); shared with analytics, advertisement and marketing companies for service/platform improvement, marketing, advertising and promotions (all platforms, eSanjeevani uses analytics for non-commercial purposes only), legal compliance, law enforcement and regulatory requests (all platforms); business transfers including corporate restructuring, mergers and acquisitions (all platforms, not applicable to eSanjeevani); data security; and research purposes (most platforms for internal and marketing research. Only eSanjeevani restricts research to public health purposes). Platforms, such as Apollo 24/7, Netmeds, PharmEasy, Tata 1mg and Practo, specifically mention cross border transfer of data.

Tata 1mg maintains the most expansive data-sharing policy due to its vast intra-group ecosystem. On the other hand, eSanjeevani adopts the most restrictive approach, limiting disclosures to non-personal data for academic and public health research. However, eSanjeevani mention that data can be shared with "persons carrying out the intended medical and administrative interventions." The term "administrative interventions" is too broad and vague to constitute a clear and specific purpose.

An analysis on the clarity of disclosure on third-party data sharing, several common themes emerge. *First,* Tata 1mg, Practo, Netmeds, Lybrate and Apollo 24/7, often employ broad catch-all terms, such as 'affiliates', 'business transfers', 'partners' and 'need-to-know' basis, that obscures the identities of actual data recipients. *Second,* purposes for third-party data sharing are often bundled and vaguely described. None of the platforms, except eSanjeevani, categorise purposes into primary purposes of service delivery and secondary purposes, including analytics, marketing and advertising purposes. *Third,* none of the platforms map data points to specific recipients and for specific and differentiated purposes of sharing. *Fourth,* none of the Platforms seek granular consent for third-party data sharing, particularly

for analytics, marketing and advertising purposes. Though MedPlusMart, Lybrate and Practo allow users to opt-out of personalised marketing, advertisement, and promotional outreach.

In addition to the findings that are common across platforms, discussed above, we identified some concerning practices unique to one or two platforms. *First,* PharmEasy and Practo specifically state that they sell user data in de-identified and aggregated form, without explicit user consent, and they also do not disclose the standards of de-identification/anonymisation they use. MedPlusMart explicitly forbids sale of personal information. The rest of the platforms don't mention anything regarding sale, i.e. neither confirm nor deny it. Sale of user data without specific consent violates users autonomy and is a significant privacy risk, especially if de-identification and anonymisation is not done in a robust manner. *Second,* MediBuddy shares personal information with employers, on receipt of a formal request from the employer and upon receipt of necessary approval(s). However, no mention of explicit user consent is made or any opt-out mechanism offered for this purpose. This potentially violates the right to privacy at the workplace and renders users vulnerable to workplace discrimination on the basis of health status. *Third,* MediBuddy and PharmEasy, subject to applicable law, reserve the right *"in our sole discretion,"* to transfer personal information to any other corporate body located in India or any other country. *Fourth,* MedPlusMart: states that it may share personal information with affiliates or partners, who may then target the users for marketing, unless users actively opt-out, but how such opt-out/consent is managed is unspecified.

We also analysed if the platforms specifically mentioned that third-party data sharing is subjected to contracts to ensure confidentiality, privacy and data security. Practo, Tata 1mg, and Apollo 24/7 are the only platforms to clearly state that sharing with third parties is governed "under contract." Tata 1mg, however, also states that *"Tata Group Entities and Partners may have privacy practices that differ…"* This shifts responsibility away from 1mg and puts burden on the user to evaluate privacy risks. Netmeds also indicates that third parties may be "bound by reasonable confidentiality obligations and or generally follow accepted industry and security standards, with-respect-to the information shared. PharmEasy states that it "ensures" that third parties have implemented adequate data security measures and that they do not further disclose the data. Lybrate, MediBuddy and MedPlusMart do not explicitly mention contracts or third-party data protection assurances. eSanjeevani mentions sharing users data with persons for treatment and administrative interventions, but does not specify whether these parties constitute data processors under a valid data processing contract or agreement. Further, no platform provides the actual content or details of the contracts, other mechanisms or arrangements with third-parties publicly. No policy guarantees technical or audit mechanisms to ensure the adequacy of third-party measures. No policy mentions that the users will be notified when the data is shared or when the recipient changes. The platforms only provide a general assurance that third parties must uphold reasonable confidentiality and data security measures, which is a compliance and transparency gap.

With particular respect to data sharing with third-party analytics and advertisement companies, all platforms, except eSanjeevani engage in it. As discussed in the section on disclosures about data collection, all platforms collect detailed usage, device, network and

browsing data via cookies, including third party cookies/trackers for the purposes of analytics to understand user behaviour, categorise users and create detailed profiles. This analysis in turn, is used to personalise content and recommendations, serve targeted advertisements and optimise wider marketing efforts. Some of the practices disclosed that are of concern are:

a) Targeted advertisement, retargeting and SDK based ads - PharmEasy, Practo, Apollo 24/7, Netmeds and Tata 1mg use personal and behavioural user data to deliver targeted ads, retarget users across sites, and /or integrate third-party advertising SDKs directly into their mobile apps or websites. This means that users browsing habits, search history, product/cart information and device details are shared with ad-tech companies. Users might be "retargeted" i.e. reminded about medicines left in their cart or previous consultations etc. SDK based ads allow third parties deep technical access within the app, which may include sensitive usage data. This is high risk because profiling for ads can reveal sensitive health needs. Exposure to multiple analytics/advertiser databases increases re-identification risks. If consent is not specific and unbundled, users may not even realise the breadth of tracking and sharing taking place. In the technical analysis, trackers such as GoogleAdservices, Facebook ads, Criteo and Bing were identified. These trackers can be configured for retargeting purposes, and were found in all web platforms except eSanjeevani.
b) Session replay analytics - PharmEasy, Practo and Tata 1mg embed third party analytics that record detailed information about user interactions and transmit session details to outside vendors. Session replay can inadvertently capture personal identifiers or sensitive health queries, if not carefully masked or filtered. In the technical analysis, Microsoft Clarity, FullStory and Hotjar were the session replay analytics tools that were identified in the web platforms.
c) Loyalty and reward data sharing - Tata 1mg may share users purchase, demographic, and behavioural data with third-parties offering rewards or discounts. Such loyalty program data tends to be cross-referenced and reused by multiple companies increasing exposure. If not strictly anonymised or limited, this extends user profiles across many commercial platforms without explicit, purpose-specific consent.
d) Marketing agency sharing - Netmeds, Practo, Tata 1mg, Apollo 24/7 (via remarketing partners) share user data with marketing agencies, without explicit user consent. This may enable profiling and targeting related to sensitive health needs, raising ethical and legal risks.

With respect to disclosures on and user consent for third-party trackers our legal analysis found that: *first,* some web platforms do not specifically state the use of third-party cookies/trackers in their privacy policies. However, findings from the technical analysis reveals that all commercial platforms have third party trackers (See Table 5 below). *Second,* Detailed lists of tracker names and vendor domains are not present in any privacy policy. However, our technical analysis reveals that Google, Microsoft and Meta are the most common. *Third*, out of the eight commercial web platforms, only Netmeds provides a cookie consent banner. Some web platforms - Lybrate, Netmeds, PharmEasy and Tata 1mg - inform

users that they can restrict cookie use via their browser settings, but this passes the burden on to the users and despite turning off the cookies, some data may still be collected.

Findings of the technical analysis on data sharing via third-party trackers

Our technical analysis reveals critical gaps and privacy risks related to the deployment of third-party cookies and trackers in all eight commercial web platforms (see findings at Table 5). As discussed above, some platforms do not specifically disclose the existence of third-party trackers in their privacy policies. Some platforms mention third-party cookies/trackers but do not specifically disclose the names of the trackers or the third parties deploying them and do not mention cookie consent banners. Our technical analysis fills some gaps and compliments the legal analysis and confirms that: *first,* there is widespread use of third-party trackers by all commercial platforms. *Second,* all platforms collect and transmit data via cookies/trackers without explicit user consent. Netmeds is the only platform that displays a cookie consent banner but rather inadequately. The Data collection cookie consent banner appears on the landing page. It clearly states that cookies are used 'to enhance your user experience', offers two visible options ('Accept' and 'No, thanks'), and links to 'More info', which takes users to the privacy policy for further details. However, the banner is limited as it does not disclose which types of cookies are being used (for example, strictly necessary, analytics, or advertising cookies), does not offer a way to provide granular consent for different categories and does not specify which third parties will receive the data. *Third,* the dominant third party recipients of data are Big Tech, such as Google, Microsoft and Meta - entities that operate large-scale behavioural advertising and analytics infrastructures. This means that users' health-related activities on Indian telemedicine platforms are being shared with global ad-tech systems, creating long-term privacy risks. *Fourth,* the data being transmitted, without explicit user consent, include sensitive personally identifiable information including, health categories and symptoms, user phone numbers, location data, medicines and diagnostic tests selections, teleconsultation requests, user navigation behaviour and detailed page interactions.

Table 5: third-party trackers in telemedicine platforms

#	App Name	Type of Data Shared	Third Parties Receiving This Data
1	Tata 1mg	Teleconsultation request, Indication searched, Medicine name, price, manufacturer	Google Analytics, AdRoll, DoubleClick, Bing, Fullstory, Facebook
2	Lybrate	Location, Consultation request, Indication (e.g., acne, pimples)	Google Analytics
3	Apollo 24/7	Specialty & symptoms, Doctor's name (teleconsultation), Phone number	Google Ads, Microsoft Clarity

Table 5: third-party trackers in telemedicine platforms			
4	Practo	Location, Phone number, Health category & sub-category	Google Analytics, Google, AdRoll, Bing (Microsoft)
5	Netmeds	Medicine category, name, price, manufacturer	Google, DoubleClick, Facebook
6	PharmEasy	Diagnostic test name, Medicine selection, Page selections	Google Analytics, Criteo, DoubleClick, Dotomi
7	MediBuddy	Medicine name, Landing on doctor & lab test pages	Google Analytics, Google Maps, New Relic
8	MedPlusMart	Location, Medicine name, price, manufacturer; Lab test details; Navigation history	Google Ads, DoubleClick, Google Analytics, Google Ad Service
9	eSanjeevani	User landing on Website homepage	Twitter

Sharing identifiable user information, such as phone number, city, and sensitive health-related concern categories (e.g. depression, anxiety, sexual and reproductive health concerns, skin concerns etc.) - with third-party advertising and analytics platforms (Google, AdRoll, Bing, etc.) without specific user consent has serious privacy, ethical, and legal implications and is violative of consent and privacy standards. These platforms collectively receive around 7 crore monthly visitors, many of whom are active users, making the scale of privacy violations quite substantial. The users may never know their health concerns have been shared with third parties and can be linked to their IP addresses, mobile numbers and location, enabling profilign, racking and sharing for targeted advertising or analytics.

5.1.8 Right to withdraw consent

Eight of the nine telemedicine web platforms explicitly recognise users' right to withdraw consent. Only eSanjeevani does not expressly specify the right. Five websites, including Tata 1mg, Lybrate, Apollo 24/7, Practo and MediBuddy, provide a specific email address to process the request for withdrawal. PharmEasy provides generic email instructions without a specific email address to communicate the withdrawal. Netmeds and MedPlusMart state the right but offer no guidance on how to exercise it.

5.2 Privacy principles

5.2.1 Purpose limitation

Though the privacy policies broadly disclosed the purposes of data collection, processing and third-party sharing, we analysed the policies to see if they meet the principle of purpose limitation. We first examined whether the privacy policies contain specific purposes for which users' data can be used. Of the nine, five web platforms - Netmeds, PharmEasy, eSanjeevani, Tata 1mg and Practo - provide an inclusive or exhaustive list of purposes for which users' data can be used. Of these, Practo provides the most detailed and specific list. In other cases, however, the purposes are stated in broad terms. For example, Tata 1mg states users' data can be shared for service and contractual obligations without specifying what they entail. On the other hand, the remaining four apps - Lybrate, Apollo 24/7, MediBuddy and MedPlusMart - provide an exclusive or illustrative list of purposes.

We analysed if the purposes mentioned are clear and specific. As mentioned in the section on disclosure of purposes, we found that most web platforms list vague and overbroad purposes without the necessary specificity and fail to clarify the specific nature or scope of processing. This violates the legal requirement for clear and specific purpose. Further, they also use catch-all future expansion clauses enabling unspecified future use without re-consent. Commercial platforms embed vague and overbroad phrases or catch-all future use clauses that allow indefinite present and future use without user consent and control, thereby permitting function creep and violating principle of purpose limitation.

Other factors that violate principle of purpose limitation are: bundling of primary purposes with other purposes, particularly analytics, advertising, marketing and commercial research; not mapping specific categories of data to specific purposes for processing and sharing with third-parties; not clearly mapping use of personal data and anonymised data for specific purposes for processing and sharing with third-parties.

5.2.2 Data minimisation

The section on disclosures related to data collection in the notice and consent section, explains the data collection practices of web platforms and highlights the unique data points collected by the platforms. The principle of data minimisation applies across data collection, processing, and sharing of personal data. We analysed the data collection practices and found non-adherence to principles of data minimisation and purpose limitation, with respect to broad practices applicable to all web platforms and some specific practices unique to some web platforms.

The broad findings applicable to every platform include: *First,* none of the platforms specifically state that they adhere to the principle of data minimisation and collect only the data necessary for their services. *Second,* though the platforms disclose the data collected by them, there is some over-breadth (e.g., *"any detail relating to the above categories"* or *"any of the information received under…"*), which risks non-compliance with strict data minimisation. *Third,* none of the platforms map the data collected to specific purposes for

processing and sharing, and don't facilitate granular explicit user consent according to the purposes of data collection and sharing, especially for profiling, marketing and advertisement purposes, undermining data minimisation. *Fourth,* all platforms use their own cookies and also third-party cookies/trackers, which collect data across categories for a range of purposes. However, none of the platforms categorise strictly necessary cookies/trackers from ones used for analytics, profiling and marketing purposes. This would facilitate users from consenting to data collection only for essential functions. In another example, all platforms collect and share detailed device information, but do not map them to core purposes like security/fraud detection and other purposes, including tracking and profiling, which should not be collected without explicit user consent. Similarly, while payment processing requires some financial data, collecting and storing excessive details can exceed minimum requirements and increase security and privacy risk. Further, almost all platforms collect search and browsing history, not just of their website but also of any website visited before theirs, without clarifying why this is collected and retained for how long.

In addition to the findings applicable to all platforms, we identified patterns of data collection specific to one or more platforms that could be excessive: *First,* collection of location data by default unless the user disables it Practo, Lybrate and MedPlusMart. *Second,* permission for camera, microphone, contact book access (Lybrate, Tata 1mg) are privacy intrusive and often unjustified unless specifically purpose-bound to in-app video calls or upload features and specifically consented to. In any case, contact book access is not justified for core health service delivery functions. *Third,* permission to access photo gallery, SMS, bluetooth, wifi (Tata 1mg, MediBuddy) are often unnecessary for core health service delivery functions, unless purpose-bound and specifically consented to. *Fourth,* collection of sensitive demographic information - religion, ethnicity, marital status (Tata 1mg) - are not required for telemedicine and can enable profiling or discrimination. *Fifth,* MediBuddy links users to HealthKit or wearable data. It may be permissible if user-initiated or specifically opted in and consented to. But default collection and shifting the burden on the user to opt-out, is excessive data collection. *Sixth*, collection of PAN by Apollo 24/7 may be excessive, unless for specific tax-related services, like insurance reimbursements, which is not specified. *Seventh*, collecting family members and dependents personal information by MediBuddy is not justified for core health services. It raises risks if their consent is not individually obtained, or the user does not have legal authority to consent on their behalf. *Eight*, collection of sexual orientation data should only be permitted for health care service delivery and healthcare context. *Ninth,* data like biometrics collected by Apollo 24/7 and Practo should only be requested where strictly mandated by law.

5.2.3 Storage limitation

Tata 1mg, Netmeds, Apollo 24/7, Practo and MediBuddy store personal information as long as required to provide services/fulfill purpose to the user or as required by law. MediBuddy also stores user data after the retention period, for legal, tax and regulatory purposes. Similarly, PharmEasy and Practo store personal information indefinitely after it is anonymised. PharmEasy specifically mentions sensitive personal data, stating it is destroyed or anonymised as soon as purpose is fulfilled or retention is no longer necessary, while

non-sensitive details can be retained for ongoing business purposes even after the expiry of the retention period. eSanjeevani stores information for as long as the user account is in existence or according to Telemedicine Practice Guidelines or till any academic, medical, public health or administrative intervention is completed. MedPlusMart and Lybrate are silent on their data retention practices.

5.2.4 Accuracy

Other than MedPlusMart, all websites provide users the option to correct or update their personal information, while placing the onus of ensuring accuracy on the user. PharmEasy, Apollo 24/7 and Practo warn that unverifiable or incorrect information may lead to denial, and may be refused or limited if it infringes on others rights, is part of ongoing legal proceedings, is opinion-based entries or is already de-identified. MedPlusMart is silent on this parameter.

5.2.5 Data security

All nine platforms acknowledge data security in some form, but most do so with broad assurances of *"policies and measures"* rather than naming specific safeguards. Tata 1mg, MedPlusMart, Lybrate, Apollo 24/7 and Practo rely on generic pledges around secure networks and organisational measures, whereas Netmeds (firewalls and TLS), PharmEasy (encryption software and IT security techniques), and MediBuddy (SSL certificate) cite concrete technologies. Netmeds, MedPlusMart, Lybrate, PharmEasy, Apollo 24/7 and Practo explicitly reference access control, but only PharmEasy and Practo go further by advising users to safeguard their passwords. Meanwhile, all providers, except Tata 1mg and eSanjeevani, disclaim responsibility for data breaches.

5.3 User rights

Across the selected telemedicine web platforms, user rights are unevenly articulated, with commercial web platforms generally offering stronger recognition than the only public platform, eSanjeevani. Of the nine platforms reviewed, eight, excluding Netmeds, recognise the rights to access, erasure, and rectification of personal data. However, eSanjeevani confines the exercise of these rights to registration-related information. Eight of the nine platforms, including Tata 1mg, Netmeds, MedPlusMart, Lybrate, PharmEasy, Apollo 24/7, Practo and MediBuddy, suggest that users can object to the processing of their data through the option to withdraw consent. Of these, five platforms, including Tata 1mg, Netmeds, MedPlusMart, PharmEasy and Practo, also provide explicit mechanisms, including unsubscribe links, SMS opt-out options and account-level toggles, to opt out of direct marketing. None of the platforms specify the rights to information about automated decision-making, seek explanation and object to automated decision making, data portability and nomination.

5.4 Transparency and accountability

Among the nine telemedicine platforms reviewed, disclosures around privacy governance remain uneven and largely inadequate. Only three platforms, Netmeds, Lybrate, and

PharmEasy, acknowledge cross-border data flows, while none provide information on breach notification timelines. Contact details for Data Protection Officers (DPOs) are available in four cases, though Tata 1mg offers only a generic contact. Grievance Redressal Officer (GRO) details are more commonly disclosed, with eight platforms providing them. Notably, Practo, MediBuddy, and eSanjeevani list the same individual or contact point for both DPO and GRO roles, suggesting a consolidation of accountability functions. However, none of the platforms describe a formal grievance redress process. Seven platforms mention mechanisms for updating privacy notices or consent terms, but Netmeds and PharmEasy do not. In all cases, the onus remains on users to proactively monitor changes to privacy policies, with no commitment from platforms to notify users of updates.

6 Discussion

Our analysis of nine telemedicine web platforms reveals a consistent pattern of privacy governance gaps across five domains: (i) consent mechanisms that are vague, bundled and non-granular; (ii) excessive data collection; (iii) opaque third-party data sharing; (iv) vague and permissive privacy policy language; and, (v) incomplete recognition of user rights. While these issues are not unique to telemedicine platforms, their presence in a sector handling sensitive health data raises acute concerns under both ethical and legal frameworks in India. These findings align with broader critiques of India's digital services ecosystem, where commercial imperatives frequently override privacy-by-design principles.

6.1 Vague, bundled and non-granular consent

The study finds that consent mechanisms across telemedicine platforms are consistently vague, bundled and non-granular, offering users no meaningful control over how much of their data is collected and how it is processed. Consent is typically implied through continued use, login or registration, with no requirement for an explicit opt-in. This violates section 6 of the DPDPA, which requires that consent must be given with a clear affirmative action. Where consent prompts exist, they are often pre-ticked and include multiple purposes, such as service delivery, marketing and analytics, without allowing users to selectively opt out. This take-it-or-leave-it structure further undermines section 6 of the DPDPA, which mandates that consent must be taken for a specific purpose. Such consent mechanisms are also contrary to judicial precedents in India. The Supreme Court of India, in the landmark privacy judgment, explicitly recognised the right of users to control their personal data, including how it is collected, stored and shared. This principle directly challenges telemedicine platforms collecting personal data without specific, explicit and granular consent.[27]

The practice further violates India's competition law. In 2024, the Competition Commission of India imposed a 2.13 billion INR penalty on Meta for abusing its dominant position by enforcing a privacy policy that required users to accept data-sharing with Facebook and its affiliates (without an option to opt-out of it) as a condition for continued use of the instant

[27] *Justice K.S. Puttaswamy (Retd) vs Union of India*, *2019 (1) SCC 1*.

messaging platform WhatsApp.[28] In Appeal, The National Company Law Appellate Tribunal upheld the penalty and agreed with the CCI that the policy was exploitative and a violation of competition law because it did not give users a meaningful choice to opt put of such sharing.[29]

We also observed that telemedicine web platforms initiate the collection of users' browsing data and seek access to sensitive permissions, such as camera, microphone and location, often before any privacy notice is displayed or consent is secured. These platforms activate tracking scripts, software development kits, and analytics tools immediately upon website visits. Our study corroborates the 2023 CIS-Privacy International study that found that several Indian health applications shared sensitive health data with third-party trackers, such as Facebook and Google, before users had reviewed or accepted privacy terms.[30] Such pre-consent data collection violates informed consent as the DPDPA requires that consent be collected before or at the time of data collection. Additionally, it violates the DPDPA's requirement that personal data must be processed only on the basis of free, specific, informed, unconditional and unambiguous consent given for a specific purpose.[31] Taken together, our findings suggest that consent on Indian telemedicine web platforms is more tokenistic than substantive, serving as a legal fig leaf rather than a genuine safeguard of user autonomy.

6.2 Excessive data collection

Our analysis reveals that Indian telemedicine web platforms routinely collect far more personal data than is necessary for the provision of health services, in clear tension with the data minimisation principle embedded in DPDPA.[32] As an example, we observed that some platforms collected highly sensitive and non-essential demographic attributes, such as marital status, occupation, ethnicity and religion - categories that have no direct bearing on facilitating teleconsultation or e-pharmacy services but carry heightened risks of profiling or discrimination. Platforms also capture device and usage metadata, including IP addresses, operating system, browser type, location coordinates and unique device identifiers. Embedded third-party trackers from Google, Microsoft and Meta enable persistent device fingerprinting across sessions.

Earlier case studies and media reports corroborate our findings. For example, India's COVID-19 contact tracing app, Aarogya Setu, faced criticism for continuous collection of GPS location, Bluetooth proximity logs, mobile numbers and self-reported health status into a centralised dataset, far exceeding the minimum needed for exposure alerts.[33] Similarly, the

---

[28] Competition Commission of India, *In Re: Updated Terms of Service and Privacy Policy for WhatsApp Users Suo Motu Case No. 01 of 2021*, 2024.
[29] Internet Freedom Foundation (IFF), *Statement: The NCLAT's WhatsApp Privacy Policy Judgement is a Mixed Bag*, Internet Freedom Foundation (04 November 2025) https://internetfreedom.in/statement-the-nclats-whatsapp-privacy-policy-judgement-is-a-mixed-bag/
[30] Privacy International and Centre for Internet and Society, "The hidden cost of digital health services"available at: http://privacyinternational.org/long-read/5151/hidden-cost-digital-health-services (last visited July 16, 2025).
[31] Government of India, *Digital Personal Data Protection Act*, 2023, ss. 4-6.
[32] *Ibid.*, s. 6(1).
[33] *Aarogya Setu: What's Problematic and Why? A Privacy Rights Expert Answers*, (The Wire, 2020).

2023 CIS-Privacy International study found that Indian health apps transmitted symptom searches, prescription details, precise location data and persistent device identifiers to third-party trackers, enabling long-term profiling well beyond the scope of teleconsultation or pharmacy fulfillment.[34]

From a legal standpoint, such breadth of collection violates the proportionality doctrine which recognises that collecting extraneous data, especially in a sensitive sector such as healthcare, is neither necessary nor minimally intrusive.[35] Such breadth of collection also violates the DPDPA and the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules), both of which require that only data necessary for the specified purpose be processed.[36] Ethically, excessive data collection violates the principles of autonomy, non-maleficence, justice and trust. They strip patients of meaningful control over their data, increase the risk of harm through breaches, profiling or discrimination, and disproportionately impact vulnerable groups, especially when sensitive health data is combined with socio-economic or demographic markers. In a sector where confidentiality is foundational, opaque and intrusive data practices erode the trust essential to effective healthcare delivery.

6.3 Opaque third-party data sharing

The third-party data sharing in the selected telemedicine web platforms is not a marginal occurrence but it is built into the very architecture of most platforms. The technical analysis of the study shows that commercial providers routinely embed external software development kits, analytics tools and advertising trackers for companies, especially Big Tech firms such as Google, Meta, Microsoft and Amazon Web Services. These integrations allow sensitive health data, device identifiers and behavioural metadata to flow to entities that are not directly involved in delivering care. Persistent identifiers, such as advertising IDs, are shared alongside sensitive health data, enabling long-term cross-platform profiling.

The CIS-Privacy International study, which documented how Indian health apps transmitted symptom searches, prescription details and precise location data to third-party trackers, such as Facebook and Google, corroborates the findings of this study.[37] These companies are likely to re-share the sensitive information with an even wider network, enabling granular profiling which can be misused by insurance companies, employers and advertising firms.[38] A 2021 study on Indian healthcare apps warns that combining sensitive health information with persistent device identifiers produces datasets that are both highly valuable to commercial

---

[34] Privacy International and Centre for Internet and Society, "The hidden cost of digital health services"*available at*: http://privacyinternational.org/long-read/5151/hidden-cost-digital-health-services (last visited July 16, 2025).

[35] *Justice K.S. Puttaswamy (Retd) vs Union of India*, *2019 (1) SCC 1*.

[36] Government of India, *Digital Personal Data Protection Act*, 2023, s. 6(1); Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011, rule 5.

[37]Privacy International and Centre for Internet and Society, "The hidden cost of digital health services"*available at*: http://privacyinternational.org/long-read/5151/hidden-cost-digital-health-services (last visited July 16, 2025).

[38] Quinn Grundy et al., "Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis" *BMJ* l920 (2019).

actors and extremely difficult to anonymise.[39] In low- and middle-income countries, these integrations often proceed without rigorous due diligence, leading to data flows that undermine domestic privacy laws as well as accepted norms on patient confidentiality.[40] In the Indian context, third-party data sharing practices of telemedicine web platforms raise serious proportionality and purpose limitation concerns under the DPDPA and SPDI Rules.[41]

Critically, these practices do more than threaten individual privacy. They consolidate market power of a handful of global technology corporations. By embedding their analytics and advertising infrastructure within Indian telemedicine platforms, Big Tech firms position themselves as indispensable intermediaries in the country's digital health ecosystem. Scholars describe this as data colonialism or the large-scale appropriation of human life through data extraction, mirroring the extractive logics of historic colonialism through digital infrastructures.[42] In the health sector, these arrangements risk entrenching digital health coloniality, i.e. a political economy in which local health systems become dependent on foreign-owned digital infrastructure while the economic and strategic value generated from local populations' data accrues elsewhere.[43]

6.4 Vague privacy policy language

The study highlights that the privacy policies and/or consent notices of Indian telemedicine web platforms are often couched in vague, open-ended and imprecise language while describing what data is collected, how it will be used and with whom it will be shared. Common patterns include broad phrases, such as 'for improving our services', 'for research purposes' and 'for marketing and promotional activities' without defining the scope or duration of these purposes. These policies often refer to 'affiliates', 'partners' or 'third parties' without actually naming the recipients of user data. Such language lumps together essential processing with optional or commercially motivated uses, making it difficult for users to distinguish between what is necessary and what is not.

This vagueness undermines the ability of average users to make informed decisions and creates information asymmetry: the platform knows exactly it will use personal data but the user is left guessing. Legal scholarship has long stressed that clarity and precision are essential to the rule of law.[44] In other words, contracts must be written with sufficient clarity and precision that people can reasonably predict how they will apply in practice. Similarly,

---

[39] Prathamesh Churi, Ambika Pawar and Antonio-José Moreno-Guerrero, "A Comprehensive Survey on Data Utility and Privacy: Taking Indian Healthcare System as a Potential Case Study," 6 *Inventions* 45 (2021).
[40] Anubhuti Sood et al., "Challenges and recommendations for enhancing digital data protection in Indian Medical Research and Healthcare Sector," 8 *npj Digital Medicine* 48 (2025).
[41] Government of India, *Digital Personal Data Protection Act*, 2023, ss. 5 & 10; Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011, rule 6.
[42] Nick Couldry and Ulises Ali Mejias, "The decolonial turn in data and technology research: what is at stake and where is it heading?," 26 *Information, Communication and Society* 786–802 (2021); Nick Couldry and Ulises Ali Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject," 20 *Television and New Media* 336–49 (2018).
[43] Sharifah Sekalala and Tatenda Chatikobo, "Colonialism in the new digital health agenda," 9 *BMJ Global Health* e014131 (2024).
[44] Paul Craig, "Legal Certainty and Legitimate Expectations," 2nd ed. *EU Administrative Law* 549–89 (Oxford University PressOxford, 2012).

opacity in data practices compounds the power imbalance between data fiduciaries and data principals, making rights rhetorical rather than real.[45] Vagueness in privacy policies may also fall foul of the DPDPA as it will impede meaningful enforcement of recognised principles, including consent, purpose limitation and data minimisation, exercise of rights by data principals and access to grievance redress. In short, vagueness is not a mere drafting flaw but a substantive governance problem.

6.5 Incomplete recognition of user rights

The study notes that basic user rights, including the rights to access information about, erasure and rectification of personal data, are acknowledged by nearly all telemedicine platforms. However, none offer a meaningful pathway for the exercise of these rights through clear instructions on how to submit a request, what identity documents are required or what form the request should take. In particular, the contact details of DPOs and GROs are often confined to a single, generic email address buried in lengthy policy text, with no published telephone numbers, office addresses or escalation hierarchy. Crucially, no platform recognises the right to receive information about or challenge automated decision-making, data portability and nominating a representative. By failing to articulate clear procedures, timelines and points of escalation, telemedicine platforms reduce statutory rights to paper promises.

6.6 DPDPA limitations

As noted in the preceding sections, the selected telemedicine web platforms are deficient in ensuring data protection and upholding patient privacy. These deficiencies will need to be addressed as and when the DPDPA comes into force. That said, the DPDPA, while establishing a framework for digital data governance, contains several gaps of its own.

Opacity in third-party data sharing

Section 5 of the DPDPA substantially weakens the scope of the notice obligation. In contrast to data protection laws in other jurisdictions (See table 1), and even India's draft Personal Data Protection Bill of 2019, the DPDPA does not obligate data fiduciaries to disclose to individuals information of third parties with whom their personal data may be shared.[46] The SPDI Rules, imposed a more rigorous standard by requiring data fiduciaries collecting sensitive personal data to inform individuals about the intended recipients of such data.[47] The repeal of this obligation has, therefore, lowered rather than raised the level of protection available to individuals. The erosion also runs counter to the constitutional benchmark articulated in *Justice K.S. Puttaswamy v Union of India*, which emphasised that meaningful consent is inseparable from transparency and that individuals must be informed about how and where their data will be used or transferred in order to exercise genuine decisional autonomy.[48]

---

[45] Daniel J. Solove, "A Taxonomy of Privacy," 154 *University of Pennsylvania Law Review* 477 (2006).
[46] Government of India, *Personal Data Protection Bill*, 2019, s. 7(1).
[47] Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011, rule 5(3)(c).
[48] *Justice K.S. Puttaswamy (Retd) vs Union of India*, *2019 (1) SCC 1*.

The absence of clear disclosure requirements around data-sharing arrangements carries significant consequences. Without transparency, individuals are unable to grasp the full extent of how their personal information, especially sensitive health data, may be processed, leaving them with an illusory sense of control over their privacy. When the identity of downstream recipients is concealed, data may end up in the hands of actors to whom individuals would never have granted consent, creating opportunities for misuse, including constructing granular profiles of users which are then leveraged for targeted advertising and other profit-driven activities.

The findings of this study, together with earlier studies, substantiate these concerns.[49] Such data-sharing practices also explain the emergence and dominance of Big Tech firms.[50] However, rather than rectifying the opaque data sharing arrangements between telemedicine web platforms and technology companies, the DPDPA leaves them largely intact by neither imposing a duty to reveal them nor guaranteeing individuals the ability to opt out of them. While our study notes voluntary opt-out options in the privacy policies of some telemedicine web platforms, such measures cannot be regarded as substitutes for a statutory guarantee under the DPDPA. This is because voluntary measures are discretionary, unevenly implemented and unenforceable in the absence of regulatory oversight. This undermines the right to informational privacy of individuals.

Non-recognition of crucial rights

In international debates on the regulation of digital technologies, certain rights have increasingly been recognised as essential to safeguard. In contrast to the DPDPA, modern privacy legislations in other jurisdictions (see table 1) explicitly recognise the rights to seek information about automated decision-making, seek explanation and object to automated decision-making, object to processing of personal data for specific purposes, including marketing and data portability.

First, automated decision-making and profiling are increasingly deployed in healthcare settings from diagnostic tools to insurance claim processing to premiums.[51] In contexts where decisions directly affect access to treatment or coverage, the absence of the right to be informed directly impedes an individual's ability to seek human reviews or challenge automated outcomes, while an absence of the right to object to automated decision-making hinders an individual's choice not to be subjected to it. Yet, the DPDPA provides no such guarantees, leaving telemedicine users vulnerable to unreviewable algorithmic determinations.

---

[49] For example, see Privacy International and Centre for Internet and Society, "The hidden cost of digital health services"*available at*: http://privacyinternational.org/long-read/5151/hidden-cost-digital-health-services (last visited July 16, 2025).

[50] Kean Birch, Dr Cochrane and Callum Ward, "Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech," 8 *Big Data & Society* 20539517211017308 (2021).

[51] Rajendra Pratap Gupta, "India's AI Healthcare Revolution: How Doctors, Hospitals, MedTech, and Pharma Are Leading the Future of Digital Health" *ET Healthworld* (India, 19 April 2025); David S. Greenberg, "Health Insurers Sued Over Use of Artificial Intelligence to Deny Medical Claims" *ArentFox Schiff*, 2023*available at*: https://www.afslaw.com/perspectives/health-care-counsel-blog/health-insurers-sued-over-use-artificial-intelligence-deny (last visited September 26, 2025).

Second and equally concerning is the lack of a right to object to direct marketing. As discussed earlier in this section, existing evidence shows that sensitive health data is routinely commodified and shared with third parties, especially Big Tech firms, without user consent. Without a statutory right to object, patients risk profiling, manipulation and erosion of trust.

Finally, the DPDPA does not recognise the right to data portability, despite its centrality to patient autonomy and continuity of care in the digital world. Data portability allows individuals to access and transfer their health records across providers, facilitating a second opinion and proactive health management. The National Digital Health Blueprint, the Health Data Management Policy and the draft Personal Data Protection Bill explicitly recognise this right.[52] Its removal from the DPDPA represents a significant retreat from the government's own stated objectives for digitisation in healthcare.

Taken together, the absence of these rights reflects a troubling retreat from rights-based governance of digital health. For telemedicine, which involves sensitive health information, these omissions risk eroding patient trust and undermining the goals of digitisation. Therefore, recognising these rights is an imperative for a robust and rights-based environment for technological innovation.

Lack of transparency

Transparency and privacy are foundational to building trust in telemedicine services.[53] Patients disclose some of their most sensitive information in health settings. Without clear disclosures on how this data is processed and holding telemedicine platforms accountable for misuse, patient autonomy cannot be meaningfully safeguarded. The DPDPA, however, does not adequately empower users to hold these platforms accountable. For one, it leaves the design of grievance redress mechanisms to the discretion of data fiduciaries themselves, creating the risk of arbitrary or perfunctory rejection of complaints. This mirrors long-standing concerns with the health insurance sector, where companies often dismiss claims without providing reasons.[54]

Further, section 10(2)(iv) of the DPDPA compounds the problem by allowing the DPOs of significant data fiduciaries to also serve as the GROs.[55] This dual role creates an inherent conflict of interest: the same official responsible for ensuring compliance would adjudicate complaints of non-compliance. In effect, the DPO becomes the regulator and the respondent, undermining the credibility and independence of the grievance process.

---

[52] National Health Authority, *National Digital Health Mission: Health Data Management Policy*, 2021; Government of India, "National Digital Health Blueprint" (Ministry of Health and Family Welfare, Government of India, 2019); Government of India, *Personal Data Protection Bill*, 2019, s. 19(1).

[53] Salvador Tarodo Soria, "Patient autonomy in the context of digital health," 39 *Bioethics* 404–13 (2025); Steven M. Williamson and Victor Prybutok, "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare," 14 *Applied Sciences* 675 (2024); Ravi Gupta et al., "Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information," 6 *JAMA Network Open* e231305 (2023).

[54] Shefali Malhotra et al., "Fair Play in Indian Health Insurance" (NIPFP Working Paper No. 228, 2018).

[55] section 10(2)(iv) of the DPDPA…

Beyond redress, the DPDPA falls short on transparency obligations. Apart from limited provisions on third-party data sharing, data fiduciaries are not required to proactively disclose critical information such as their rights recognised under DPDPA, updates to privacy policies, the process to be followed in the event of a data breach or details of cross-border transfers. The absence of these obligations weakens the ability of individuals to exercise autonomy over their health data and enforce their rights meaningfully.

No requirement of a privacy policy

The DPDPA does not specifically require data fiduciaries, including telemedicine platforms, to publish a privacy policy. This is a significant omission, especially in the present context where sensitive health data is routinely processed. While both a privacy policy and a notice for consent are essential for ensuring transparency and protecting user privacy, they serve distinct functions. A privacy policy is a comprehensive document that explains how an organisation collects, uses, manages, and safeguards personal data, thereby informing individuals of its overall data practices. In contrast, a notice for consent is tied to a specific instance of processing and seeks explicit permission for that activity.

Earlier frameworks in India recognised this distinction. The SPDI Rules mandated both a privacy policy and a consent notice, while the draft Personal Data Protection Bill 2019 went further by introducing a "privacy by design policy" within a dedicated chapter on transparency.[56] However, subsequent iterations of the legislation diluted these requirements. The risks of such omissions were evident during the COVID-19 pandemic, when the CoWIN vaccination platform initially lacked a privacy policy until the Delhi High Court directed its publication.[57] Given this precedent, it would be reasonable to expect that the DPDPA would mandate privacy policies as a baseline safeguard. Yet, it fails to do so.

7 Conclusion

Taken together, our findings and discussion demonstrate a consistent pattern that while telemedicine platforms present themselves as expanding access to health services, their data practices fall short of legal standards of meaningful consent, transparent data processing and safeguards against opaque third-party data sharing. The gaps we identified - implied and bundled consent, excessive data collection, broad and vague purposes for data processing and sharing, and commodification of health data - undermine the legal standards of user autonomy, privacy by design, data minimisation and purpose limitation. In doing so, they violate the right to confidentiality and privacy of sensitive health data, a cornerstone of the right to health and public health practice. These systemic weaknesses also highlight some regulatory blind spots in the DPDPA that fail to adequately protect users autonomy and privacy, making individuals vulnerable to harms arising from unauthorised or unexpected use of their health data by telemedicine platforms and third parties.

---

[56] Government of India, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011, rules 4 and 5; Government of India, *Personal Data Protection Bill*, 2019.

[57] Vipin Sanghi and Jasmeet Singh, *Manisha Chauhan vs Government Of Nct Of Delhi- & Anr*, 2021.

Against this backdrop, the conclusion section makes concrete recommendations for the telemedicine platforms to align their privacy policies and data governance mechanisms with the DPDPA as well as global best practices. The conclusion also recommends measures that the Government of India needs to adopt for clearer standards, stronger enforcement mechanisms, and accountability structures.

7.1 Recommendations for web platforms

Web platforms must make changes to align their data collection and processing practices with the DPDPA, the *Puttaswamy* judgment and globally recognised best practices These include the following.

Rewrite privacy policies for accessibility:

a) Use clear, plain and non-legalistic language for easy readability and understanding.
b) Display the privacy policy at a prominent place on the platform to increase its visibility before login or registration.
c) Provide privacy policy/notice for consent in multiple Indian languages.
d) Implement audio and screen-reader-friendly versions for persons with disabilities to ensure compliance with the Rights of Persons with Disabilities Act, 2016.

Strengthen consent mechanisms:

a) Establish mechanisms to ensure that opt-in consent is collected by an explicit, affirmative action before or at the time of data collection and processing.
b) Move away from bundled consent. Introduce explicit, granular opt‑in for distinct purposes such as healthcare delivery, marketing, and third‑party data sharing.
c) Clearly mention the process of withdrawing consent in the privacy policy, and ensure that the process of withdrawing consent is as easy as giving consent.
d) Provide the contact details of the Data Protection Officer and Grievance Redress Officer in the privacy policy.

Strengthen purpose limitation and data minimisation:

a) Clearly separate primary versus secondary purposes, map data points collected as per these distinct purposes, and require specific opt-in consent for all the purposes, and especially for secondary ones (e.g., marketing, ads, analytics, research partnerships).
b) Avoid linking health data with advertising ecosystems (e.g., Google Ads, Meta Pixel), which is both unnecessary and highly privacy-intrusive.
c) Collect only what is strictly necessary for the primary purpose of service delivery, or for purposes for which specific opt-in consent has been obtained.
d) Avoid capturing sensitive demographic attributes (religion, ethnicity, marital status) unless essential and justified.
e) Avoid collecting excessive device-level signals (e.g., device identifiers, advertising IDs) unless medically essential.

Improve transparency in third-party data sharing:

a) Implement cookie consent banners with clear distinction of essential and non-essential cookies and provide option to opt-in to data sharing via third-party cookies/trackers
b) Disclose all categories of third-party recipients including cross border transfers and the jurisdiction of cloud providers, the purposes of sharing, and whether data is commodified
c) Require third-party processors to comply with purpose limitation and storage limitation norms
d) Require third-party contracts to prohibit further sharing, prohibit secondary profiling and mandate deletion after service fulfilment and align with obligations of data fiduciaries and data processors
e) Publish data-sharing agreements in summary form, showing purpose, safeguards and retention obligations

Inform about and operationalise user rights:

a) Provide clear information on the rights of users - access, correction and erasure of personal data, grievance redress and nomination, and the processes to operationalise the rights meaningfully.
b) Go beyond access, rectification, and erasure and recognise rights to data portability, objection to marketing, and safeguards against automated decision-making. Provide simple, responsive mechanisms for exercising these rights.
c) Include algorithmic transparency by disclosing when AI tools are used in triage, recommendations, or fraud detection, providing a right to explanation for users affected by automated outcomes, conduct bias audits and publishing summaries for transarency, and ensure human-in-the-loop oversight for all high-risk decisions and avoiding "black box" AI tools without auditability.
a) Strengthen accountability by appointing Data Protection Officers separate from grievance officers.
b) Provide a "Do Not Sell or Share My Data" toggle, even if the platform claims to use only "de-identified" data.
c) Provide mandatory data-breach notifications to users with clear mitigation guidance.

Strengthen security practices:

a) Disclose organisational and technical security measures in privacy policies.
b) Implement encryption at both rest and transit including for chat logs, prescription uploads, and diagnostic reports.
c) Prevent device fingerprinting unless medically justified, as it can uniquely identify users without consent.
d) Restrict sharing of IP addresses and device IDs with ad-tech or third-party analytics.
e) Conduct regular privacy/security audits, penetration testing and vulnerability assessments, and make the audit results publicly available

7.2 Recommendations for the government

Amend and strengthen the DPDPA:

a) Expand notice obligations to mandate disclosures on third party data sharing and cross border transfers
b) Explicitly require granular consent mapped out for data collection linked to specific purposes for processing and third-party sharing
c) Introduce rights currently missing, such as data portability, objection to marketing, and safeguards against automated decision-making
d) Regulate health tech surveillance, behavioural tracking, and digital fingerprinting. Issue binding rules that prohibit or severely restrict tracking pixels (e.g., Meta Pixel, Google analytics) on health platforms. Ban targeted advertising based on health conditions
e) Lay down legal thresholds and standards for de-identification and anonymisation

Implement health sector specific legal framework for health data:

a) Provide clarity on permissible primary and secondary uses of health data
b) Prohibit or limit commodification of health data including limits on sale, brokerage, or monetisation without explicit, informed consent and strong public-interest justifications.
c) Regulate cross-border transfers in the health sector with necessary disclosures, risk assessments and necessary safeguards
d) Regulate non-personal health datasets as public infrastructure undergirded by robust governance frameworks
e) Strengthen the existing health data management frameworks under the Ayushman Bharath Digital Mission.
f) Develop legal framework, or at the minimum a sector specific guidelines, for using AI technologies in the health sector. This framework should spell out explicit requirements for safety, accuracy, reducing bias, clinical validation, data governance, transparency, and accountability; as well as accountability for developers and deployers including platforms across AI lifecycle.

Revise the Competition Act:

To address data dominance and unfair privacy practices in digital health, the government should amend the Competition Act 2002. Data-driven forms of dominance, exploitative privacy practices, and infrastructure lock-ins that currently define the telemedicine and digital health ecosystem are not sufficiently addressed by India's Competition Act, 2002, despite recent amendments. Due to their heavy reliance on Big Tech clouds, analytics, and identity solutions, telemedicine platforms run the risk of market concentration, secret data sharing, and obstacles to entry for Indian competitors. In addition to distorting competition, vague, bundled, and non-granular consent practices require users to submit to privacy-invading processing in order to obtain necessary health services. Several countries have significantly revised their competition/anti-trust laws to include the following measures, which should also be considered by the government of India:

a) Introduce data and infrastructure dominance as a recognised form of market power. Equip the Competition Commission of India (CCI) to investigate not only market share, but also control over user data, the ability to profile and network effects.
b) Treat some privacy harms as anti-competition conduct, such as bundled consent, pre-ticked consent boxes, making access to essential services conditional on excessive data sharing, or using behavioural or device-level data to create barriers to entry.
c) Equip CCI to investigate digital health platforms for excessive data extraction and exploitation of users.
d) Categorise dominant cloud infrastructures, web analytics tools and AI triage or diagnostics tools as essential digital facilities and empower CCI to require measures to prevent big tech infrastructure lock-ins.
e) Empower CCI to investigate data sharing agreements to prevent concentration of health data in a few private hands.
f) Categorise dominant digital players as "gatekeepers" and impose mandatory ex ante measures on them, including prohibiting mixing of data across services without explicit consent, prohibiting tying or bundling, mandatory interoperability, restrictions on self-preferencing, transparency in advertising and data monetisation and periodic privacy-competition audits.

C-HELP | CENTRE FOR HEALTH EQUITY, LAW & POLICY

Indian Law Society
Law College Road
Pune 411004
Maharashtra, India
www.c-help.org
contact@c-help.org