Volume **8** (1) 2026 https://doi.org/10.5204/lthj.3987

Between Flow and Friction: Regulating Health Data Flows in India's National Digital Health Ecosystem

Ramya Chandrasekhar
Center for Internet and Society – CNRS, France

Abstract

Digital health infrastructures, such as India's National Digital Health Ecosystem (NDHE), are touted as the panacea for improving universal healthcare, particularly in the Global South. Central to this infrastructure is the generation and circulation of health data, i.e. digital data relating to any facet of health. This article offers two critical analyses of the NDHE – *first*, the centrality of the 'flow' of health data to enable monetisation of these data flows by commercial actors (and consequently, the commercialisation of health), and *second*, the ways in which this market-driven imaginary of the NDHE reshapes principles of data governance such as informed consent and impact assessments into negative frictions for health data flows. Finally, this article instead offers suggestions on how to implement these legal principles through friction-in-design regulations, to engineer a necessary 'drag' to limit the commodification of health data flows in the NDHE.

***Keywords**:* India; health data; data flows; friction; informed consent; impact assessment.

I. Introduction

Digital health infrastructures continue to generate excitement for their transformative impact on universal healthcare, particularly in the Global South. Central to digital health, is the generation and circulation of health data, i.e. digital data relating to any facet of health. Funders, governments, and proponents extol 'data flows' for enabling Big Data and AI in healthcare, claiming these data-driven technologies enhance healthcare access and outcomes.

On the one hand, certain health data flows are necessary. Open sharing of health knowledge artefacts – such as scholarly works, research datasets, health indicators – via digital systems can enable more research and inform policymaking. On the other hand, the increasing involvement of private sector actors because of digitalisation of health means that these actors also shape technical, legal and infrastructural aspects of *what* becomes health data and *who* benefits from this data.[1] As the introduction to this symposium collection notes, digitisation of health brings to the fore practices of exploitation, commodification and corporatisation of human data for economic gain.

However, there is a dearth of granular studies on how commercial actors shape digital health infrastructures in Global South countries.[2] Using India as an example, I examine the law and political economy of a national-level digital health infrastructure known as the National Digital Health Ecosystem (NDHE)[3]. I argue that the 'flow' of health data to enable monetisation of these data flows by commercial actors is central to the NDHE. I further argue that this political economy of the NDHE frames law as a negative 'friction' inhibiting health data flows, when in fact, laws that engender a certain amount of 'drag' in health data flows are necessary. While there are existing studies on the need for strengthening legal regulation around the NDHE particularly for health data flows, few (and often from grey literature) adopt a critical perspective to *both* law and technology

[1] Sekalala, "A Critique of Commercialization in Sub-Saharan Africa"; Fisher, "Confronting Data Inequality."
[2] Sekalala, "Colonialism in the New Digital Health Agenda."
[3] Since 2021, this infrastructure is formally referred to as the Ayushman Bharat Digital Mission.

Except where otherwise noted, content in this journal is licensed under a Creative Commons Attribution 4.0 International Licence. As an open access journal, articles are free to use with proper attribution. ISSN: 2652-4074 (Online)

© The Author/s 2026

and provide context-specific recommendations from this perspective.[4] This article seeks to fill this gap, using socio-legal desk research on regulation of health data flows combined with a simplified mock 'walkthrough'[5] of a patient using a popular digital health app in India.

This article understands health data broadly, as including personal and non-personal data, obtained from clinical as well as non-clinical settings, to the extent it relates to health and wellbeing of an individual or a populace. Section II of this article provides an overview of the components of the NDHE, the centrality of health data flows and health data monetisation to the imaginary of universal health coverage in India, and the (lack of) legal foundations for the same. Section III analyses how the political economy of the NDHE reshapes data law in its image, casting legal principles of informed consent for data flows and impact assessments for data-driven technologies as negative 'frictions.' Instead, these types of data laws should be considered as a form of 'friction-in-design' regulation, and I offer a few suggestions in this regard.[6] Section IV contains concluding remarks.

II 'Flow': The Centrality of Health Data Flows to the NDHE

In 2017, India's union government released its National Health Policy, outlining public health priorities for the coming decade. The policy identified the need to strengthen India's healthcare system – in particular, to increase access, improve quality, and lower the cost of healthcare delivery.[7] The policy also advocated for '*extensive deployment of digital tools for improving the efficiency and outcome of the healthcare system*.'[8] This now takes the shape of the National Digital Health Ecosystem (NDHE).

Launched formally in September 2021 by Prime Minister Narendra Modi, the NDHE has seen a sevenfold increase in budget allocation – from INR 30 crores in 2020, to INR 200 crores in 2024.[9] For 2025, the NDHE has received a budgetary allocation of INR 340 crores.[10] A separate regulatory body known as the National Health Authority (NHA) has also been set up to oversee implementation of the NDHE.

A. Stacking up the Various Components of the NDHE

The genesis of the NDHE lies in a consultation paper issued in 2018, where the NDHE was referred to as the 'HealthStack' - a set of foundational shared infrastructures for the generation and circulation of health data among public and private sector actors, to achieve universal healthcare coverage.[11]

[4] Radhakrishnan, "Safeguarding Patient Rights"; Chakravarthi, "NDHE - Leveraging 'Universal Health Care' for Technology and Capital?"; Jain, "Regulation of Digital Healthcare in India"; Parsheera, Private and Confidential.
[5] Light, "The Walkthrough Method."
[6] Frischmann, "Friction-In-Design Regulation."
[7] Ministry of Health and Family Welfare, National Health Policy 2017. It should be clarified that the policy sets joint priorities for both publicly funded healthcare systems as well as private healthcare facilities.
[8] Ministry of Health and Family Welfare, National Health Policy 2017, 25.
[9] Mishra, "The Ayushman Bharat Digital Mission of India"; Ministry of Health and Family Welfare, "Update on Ayushman Bharat Digital Mission."
[10] Das, "Healthcare Budget 2025."
[11] NITI Aayog, National Health Stack: Strategy and Approach.

Drawing from the HealthStack, the NDHE is comprised of four layers, as illustrated in Figure 1 below:

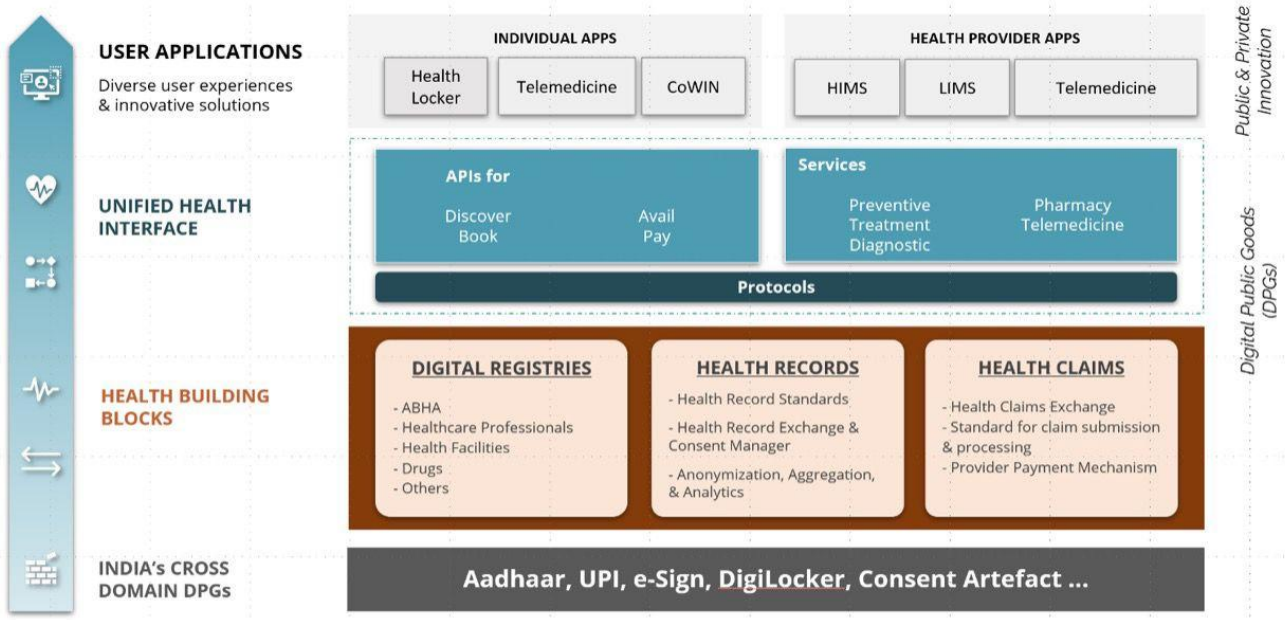


Figure 1. Architecture of the NDHE
Image: National Health Authority, https://abdm.gov.in:8081/uploads/Architecture_db6e165997.jpg.

At the base of the NDHE are pre-existing digital public goods. This includes Aadhaar (India's national biometric identification program), the Universal Payments Interface (a digital infrastructure for mobile payments) and the DigiLocker (for digital storage and sharing of documents).

Next are the foundational infrastructures for digital health – registries, standards for electronic health records, and a techno-legal architecture for consent-based sharing of health data.

Finally, there are two-interconnected layers. First, is the 'Unified Health Interface,' comprised of a set of open APIs and protocols for interoperability. Second, is the 'User Applications' layer, comprised of consumer-facing as well as healthcare-provider-facing digital health applications (or apps) that leverage the interoperability features of the Unified Health Interface.

Taken as a whole, the NDHE has been likened to a 'digital highway' that will connect different health stakeholders – public bodies, healthcare providers, healthtech companies, patients, insurance companies, regulators, policymakers, and researchers.[12] And in doing so, the NDHE will enable the circulation (or 'flow') of health data by and between these stakeholders.

B. Questionable Legal Foundations for Health Data Flows in the NDHE

At the outset, it is important to the recognise that the NDHE was launched via an executive policy, in the absence of a national personal data protection law or data governance law. Prior to the formal launch of the NDHE and after, various draft legislations on personal data protection were circulated in parliament, but were not passed.[13] In 2018, the Union Government released a draft legislation specifically for health data flows and the role of the NHA in the health information exchange, which was also not passed.[14] Instead in 2020, the NHA issued an executive policy known as the *Health Data Management Policy*, which stipulates privacy and security obligations with regard to health data flows in the NDHE.[15] This is supplemented by healthcare-related executive policies, such as the *Telemedicine Practice Guidelines, 2020* and the *Electronic Health Standards, 2016*, both

[12] See Ministry of Health and Family Welfare, "Arogya Manthan 2023 to Mark 5 Years."
[13] Kanwar, Evolution of India's Data Protection Law.
[14] *Draft Digital Information Security in Healthcare Bill, 2018*.
[15] National Health Authority of India, Health Data Management Policy, §16.

issued by the Ministry of Health and Family Welfare. But as these are non-statutory instruments, judicial enforcement is difficult.[16] Further, the absence of penalties reduces compliance with these policies.[17]

India's *Information Technology Act, 2000* imposes some obligations on corporate bodies for processing of sensitive personal data, particularly under Section 43A. A set of delegated rules specifies how these entities should handle sensitive personal data. Sensitive personal data is defined by way of an enumerated list that included data relating to: (i) physical, physiological and mental health condition; (ii) sexual orientation; (iii) medical records and history, and (iv) biometric data, but excludes any data which is freely available, accessible in the public domain, or made available under a freedom of information request.[18] Any transfer of sensitive personal data can only be undertaken with *consent* of the individual, or if the transfer is necessary for the performance of a lawful contract.[19]

In 2023, India's *Digital Personal Data Protection Act* (DPDP Act) was passed and will come into effect in a phased manner, by 2027.[20] In November 2025, the government notified delegated rules to the DPDP Act as well. Once the DPDP Act comes fully into effect, the DPDP Act will overrule Section 43A of the *Information Technology Act*.[21] In its place, the DPDP Act specifies the legal bases for processing all personal data (which will include health data), data rights and obligations for data security. As a result, the generation, use and sharing of health data by private and public actors will (eventually) need to comply with the DPDP Act.

In other words, from its inception onwards, the NDHE was being implemented in the absence of specific regulatory prescriptions on privacy and security aspects of health data flows within this infrastructure. Instead, a form of self-regulation is visible, where early adopters of the NDHE's architecture, often valorised as national champions, create their own regulatory norms for health data flows. For instance, telemedicine platforms rank their registered healthcare professionals based on algorithmic models of visibility, often using patient reviews and paid sponsorships to engineer this ranking, while offering little to no transparency about this practice. This can come into tension with (and even override) policies of statutory bodies such as the Medical Council of India, which impose restrictions on advertisements by individual healthcare professionals.[22]

C. The Centrality of Health Data Flows for the NDHE

Consider the following building blocks of the NDHE:

1. National-level registries of healthcare professionals, facilities, real-time drug stocks.[23]
2. Standards for electronic health records, including metadata and data formats.[24]
3. A unique health identifier for each individual, known as an ABHA ID.
4. A techno-legal consent framework for sharing health data.[25] Once ABHA-linked standardised health records have been generated for an individual, a consent artefact (in the form of a file packet) will be used to record the individual's stipulations for sharing of these records. Intermediaries known as consent managers will manage these consent artefacts, and use them to enable direct transfers of medical records between the entities creating these records and the entities seeking access to these records (as discussed in more detail in Section III.A below).
5. A regulatory sandbox maintained by the NHA, where healthtech players can experiment with open application programming interfaces (APIs) for interoperability between hospital information management systems and digital health apps.

Registries and health data standards in particular are necessary to modernise hospital information management systems, as well as improve visibility into the landscape of healthcare providers. But taken together, these components enable the generation of

[16] See *Syndicate Bank vs. Ramachandran Pillai and Ors*., (2011) 15 SCC 398 (holding that only executive instructions issued under statutory authority attain the force of law).
[17] Mariwala, "What Mandaviya and Vaishnaw Must Do."
[18] *Information Technology Rules, 2011*, §3.
[19] *Information Technology Rules, 2011*, §7.
[20] *Digital Personal Data Protection Act, 2023*.
[21] *Digital Personal Data Protection Act, 2023*, §44(2)(a); Ministry of Electronics and Information Technology Notification, G.S.R. 843(E).
[22] See Hunter, "Decentred Regulation," 9.
[23] Ministry of Health and Family Welfare, National Digital Health Blueprint, 2020, 7.
[24] National Resource Centre for EHR Standards, "EHR Standards for India | NRCeS"; National Resource Centre for EHR Standards, "Home - FHIR Implementation Guide for ABDM v6.0.0."
[25] National Health Authority, Health Data Management Policy, 7. For further discussion, see also NITI Aayog, National Health Stack: Strategy and Approach, 19.

health data from discrete sources – such as clinical data from healthcare facilities as well as non-clinical health data from fitness trackers and wearables – and its subsequent continuous circulation. As Fourcade and Healy note, '[i]t does not matter that the amounts [of data] collected may vastly exceed a firm's imaginative reach or analytic grasp. The assumption is that it will eventually be useful, i.e. valuable.'[26]

D. The NDHE's Focus on Digital Health Apps and the Monetisation of Health Data

Further, the NHA notes that:

> [t]he digital health landscape in India exists in siloes, which makes it difficult to search and avail services in a seamless manner. *In the current infrastructure, doctors and patients need to use the same application for a good digital experience.* As a result, a doctor does not have an easy way to let patients know how to reach them digitally; and for a patient, the discovery of a specific Health Provider is difficult as transactions and data are fragmented across different applications. *This siloed infrastructure hinders users from making optimal choices*.[27] (emphasis added)

In status quo, a single incumbent player – like a large hospital with in-house pharmacies and diagnostic centres – is therefore able to create a platform centralising access to all these services, making it difficult for smaller players to compete.

From the perspective of the Indian data market, in both cases, the generation of health data and extraction of value is siloed. As a result, the NHA seeks to create the Unified Health Interface layer of the NDHE to enable interoperability, which will enable more competition and offer more consumer choice without any 'platform-dependency' – as illustrated in Figure 2 below.

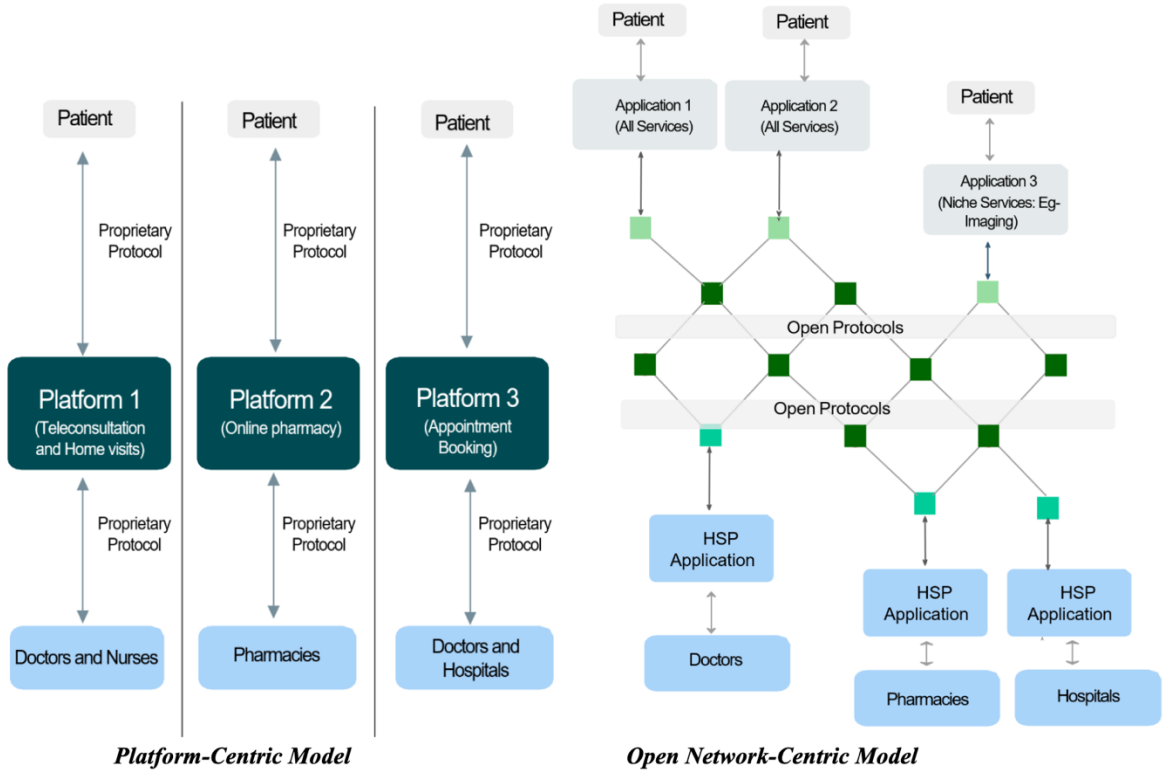


Figure 2. Comparison between the pre-NDHE and post-NDHE scenario
Image: National Health Authority. "Consultation Paper on Unified Health Interface: Synopsis." Government of India, July 23, 2021

[26] Fourcade, "Seeing like a Market," 13.

[27] National Health Authority, Consultation Paper on Operationalising UHI, 4. See also National Health Authority, Consultation Paper on Unified Health Interface.

The development of the NDHE and the Unified Health Interface needs to be analysed within India's approach to universal healthcare combined with the political agenda on data sovereignty in India. On the one hand, healthcare policy in India has moved further away from 'universal healthcare' as a public good funded by general taxes towards 'universal health coverage' where state-subsidised healthcare services are combined with public-private partnerships and enabling conditions for private investment in and private provisioning of healthcare, to offer a continuum of care for India's large population.[28] On the other hand, India's emerging data sovereignty agenda treats digital data as a national strategic asset that must benefit the Indian economy. This political agenda motivates legal and policy efforts to induce data flows at scale and make these data flows accessible to Indian businesses through interoperability standards and APIs created and maintained by the state, while at the same time restricting data flows originating within India to dominant actors outside India, namely Big Tech.[29] In fact, the NDHE is based on the Indiastack model, where e-governance initiatives such as open APIs for access to governmental systems such as the Aadhaar system render these governmental systems and data flows facilitated by them accessible to Indian entrepreneurs, to build businesses over them.[30]

In other words, the NDHE seeks to create private value from digital public goods for health. The NDHE facilitates population-scale health data flows within India to power an ecosystem of Indian digital health apps, algorithms, softwares, AI, and cloud-based services, which can ensure universal health coverage by widening consumer choice as well as bring more capital (in the form of investments) into India. Health data flows induced by the architecture of the NDHE are put in the service of the digital economy, to enrich India's software elite and healthtech startups, while India's impoverished and sick-poor citizens are reimagined as consumers and the national patient population as a 'Total Addressable Market.'[31]

For instance, Radhika Radhakrishnan points to the use of clinical and non-clinical health data by insurance companies within the NDHE, to create risk profiles for automated decision-making on insurance packages.[32] These data are also used in employee wellness initiatives in private companies, where employees share wellness data from their wearables/fitness trackers with their company and insurance companies, and this data is combined with other data to create bonuses or discounts for employees on their insurance packages.[33] The NHA has also sought fraud analytics services from private actors, where insurance claims as well as unstructured data relating to these claims (such as clinical notes) can be algorithmically analysed to validate claims filed by individual beneficiaries of government health insurance schemes.[34] In the absence of transparency and accountability obligations, impact assessments and strong legal regulations for automated decision-making, such innovations come with severe risks to fundamental rights of individuals, as has been documented in several cases around the world.[35]

Monetisation also occurs downstream.[36] A study of femtech apps revealed that widespread practice of the app developers sharing aggregated datasets of user data with third parties, and where health data then become the input for all kinds of data-driven analytics.[37] Similarly, the privacy policy of popular telemedicine apps in India, such as Practo, state that Practo can use patient data (such as demographic data, previous appointments of a patient made via Practo, data about a patient's usage of Practo services, and other data provided by a patient to Practo), to *inter alia*, contact such patient about 'new products or services.'[38] Practo's terms of service further state that Practo has the right to offer sponsored ads for clinics.[39] A combined reading indicates Practo's use of health data about a patient for the purpose of sponsored ads. In fact, Practo guarantees a minimum number of patient views for every ad paid for by a healthcare facility. With the NDHE's data standards and interoperability protocol increasingly adopted by various industry actors including Practo,[40] downstream sharing and monetisation of health data is made even easier, and is even more concerning given lack of legal regulations on the use of personal health data for targeting advertising or, until now, the lack of a personal data protection law in India.

[28] Qadeer, Universalising Healthcare in India.
[29] Pandey, India Stack; Mishra, "Data as a National Asset"; Tewari, "The Politics of Data."
[30] Samdub, "Digital Public Infrastructure" at a Turning Point; Thaker, "The New Oil."
[31] See generally, Samdub, "The State and Software Capital."
[32] Radhakrishnan, Health Data as Wealth.
[33] Radhakrishnan, Health Data as Wealth.
[34] National Health Authority, RFE: Fraud Analytics PMJAY.
[35] Dencik, "Datafication and the Welfare State"; Schäferling, Governmental Automated Decision-Making and Human Rights; Ashok, "The Curious Case of Automated Decision-Making in India."
[36] Mishra, "Femtech Apps."
[37] Chami, Data Subjects in the Femtech Matrix.
[38] Practo, "Privacy Policy", §2 read with §3.1.3.
[39] Practo, "Terms and Conditions", §4.6; "Practo Reach- A Sponsored Ad Slot for Clinics."
[40] Practo, "Practo Joins the Ayushman Bharat Digital Mission (ABDM) Ecosystem."

Finally, the continuous generation and circulation of health data creates a new form of capital.[41] The circulation of data enables assetisation, i.e. the creation of future income-streams from proprietary intangibles such as data analytics software, automated decision-making systems, or machine learning technologies.[42] And similar to Kean Birch's argument for the life sciences industry, this assetisation feeds ever-larger valuations of the healthtech industry, which in turn incentivises more investment in the sector.[43] The NDHE has been touted for making the healthcare sector 'ripe for investment,' because of "an incremental economic value of over USD 200 billion can be unlocked for the health sector [by 2031] through rigorous implementation of the [NDHE]."[44] In 2023, consultancy firm Bain & Company noted that healthtech innovations (consumer-facing and provider-facing) occupied about 25% of the entire healthcare innovation market in 2023, with a valuation of USD 7 billion.[45] With more than 10,000 healthtech startups in India as of 2024, the healthtech industry is expected to triple in value by 2028.[46]

Commercial actors also rely on these data flows to articulate visions for new markets in India. In response to a public consultation conducted by the NHA, companies such as Amazon Web Services as well as industry bodies such as NASSCOM[47], FICCI[48] and IAMAI[49], sought greater private sector involvement in the NDHE.[50] They proposed the use of cloud services for storage of electronic health records, to facilitate a market of cloud-based services for digital health.

The digitisation of healthcare in India through the NDHE to create continuous flows of health data does not necessarily ensure improved patient outcomes. Public healthcare in India remains underfunded. For instance, the National Health Policy recommended that public spending on public healthcare should account for 2.5% of Indian's annual Gross Domestic Product, but since 2017, the percentage has been less than 2%, and is now 1.94% based on the 2025 budget.[51] Further, key aspects such as ambulatory and geriatric care are absent from the 2025 budget. On the other hand, reliance on private healthcare as well as the associated costs for patients are high, while insurance coverage is low and patients who rely on public insurance schemes to access private healthcare face problems with delayed reimbursements.[52] The NDHE and its focus on creating continuous health data flows and monetising these data flows risks exacerbating the current problems that beset access to healthcare in India, as also creating new ones. For instance, Anganwadi workers (community healthcare workers) report that because of the integration of digital health apps into public healthcare schemes, they spend more time on uncompensated data work while time and quality of care work have reduced.[53]

III. Legal Frictions for Health Data Flows in the NDHE

Beyond the changes to the healthcare system that have occurred as a result of the NDHE, I argue that the NDHE reshapes legal regulations for health data flows in its image. Specifically, the NDHE casts provisions for informed consent for health data flows and impact assessments contained within the DPDP Act and the Health Data Management Policy as negative frictions inhibiting health data flows, and in doing so, weaken normative legal principles relating to informational self-determination.

A. Consent as a Techno-legal Architecture for Health Data Flows Under the NDHE

The Health Data Management Policy requires informed consent of an individual for processing their health data.[54] The DPDP Act also specifies informed consent as the legal basis for collecting and using any personal data (with exceptions where such data is collected by public bodies in certain cases).[55] The DPDP Act further specifies that consent must be 'free, specific, informed, unconditional and unambiguous with a clear affirmative action.'[56] In November 2025, the delegated rules to the

[41] Sadowski, "When Data Is Capital."
[42] Birch, "Rethinking Value in the Bio-Economy."
[43] Birch, "Rethinking Value in the Bio-Economy."
[44] Sarwal, "Investment Opportunities in India's Healthcare Sector," 6.
[45] Ghosh, "Healthcare Innovation in India."
[46] Ghosh, "Healthcare Innovation in India."
[47] National Association of Software and Service Companies, https://nasscom.in/.
[48] Federation of Indian Chambers of Commerce and Industry, https://ficci.in/api/home.
[49] Internet and Mobile Association of India, https://www.iamai.in/.
[50] Jain, "What Did FICCI, IAMAI, NASSCOM, and CII Say"; Jain, "AWS Suggests Changes to UHI."
[51] Gopal, "Union Budget 2025."
[52] Biswas, "Right to Health."
[53] Raghu, "Tamil Nadu's Anganwadi Workers"; Upadhaya, "Why The Digital Dream Soured Quickly."
[54] National Health Authority, Health Data Management Policy, §11
[55] *Digital Personal Data Protection Act, 2023*, §4(1).
[56] *Digital Personal Data Protection Act, 2023*, §6(1). Similar provisions are also contained in Section 9.2 of the Health Data Management Policy.

DPDP Act were released (DPDP Rules).[57] The DPDP Rules further elaborate on consent as the primary legal basis for personal data flows, including health data.

To operationalise informed consent, the Health Data Management Policy, the DPDP Act and the DPDP Rules encourage the use of *consent artefacts* (also known as a techno-legal consent architecture) and *consent managers* (intermediaries operating the consent artefacts) for automation of the consent process and direct data transfers between data fiduciaries.[58] The problem statement driving this consent framework is neatly captured in an executive policy released in 2017:

> Consent capture and use process is comprised of two flows: consent flow wherein consent is created and the consent parameters are shared with the relevant entities; and a data flow, where the actual data access, based on user consent, happens. In the data flow, the consent artifact is utilized to enable the data consumer to access the data held by the data provider… *The separation of the consent and data flows is a key feature of the consent framework. It is important for data flows to be executable asynchronously without the engagement of the user. This framework specifically enables this separation.*[59] (emphasis added)

Originally developed for data sharing in the payments space, this consent framework was recognised as the 'Indian Way' to break the monopoly held by Big Tech actors over data flows, while guaranteeing individual control over data flows.[60]

Consent and data flows in the NDHE: A simplified walkthrough

To understand the purported benefits of this consent framework, consider a simplified mock 'walkthrough'[61] of a patient named Maya who is using a popular telemedicine app called Practo. Maya wants an appointment with a gynaecologist to obtain birth-control medication.

Table 1: Author's visualisation of Maya's walkthrough of the Practo App

Simplified Walkthrough of Maya using Practo app ***Objective: Schedule appointment with gynecologist for birth control prescription***							
Data touchpoints	#1	#2	#3	#4	#5	#6	#7
Actions undertaken by Maya	Registration and identity verification	Locate gynaecologist and schedule appointment	Share medical records, blood pressure reading and relevant medical records with gynaecologist. Receive prescription from gynaecologist	Share prescription obtained with gynaecologist with pharmacy. Obtain medicines	Schedule diagnostic test. Share medical records with diagnostic lab	Receive test results from diagnostic lab and convey these results with gynaecologist	Claim insurance
Changes introduced by NDHE	ABHA ID	Registry of doctors	ABHA ID; Data Standards; Consent manager framework				

Maya downloads the Practo app on her smartphone. Maya is required to create an account and verify her identity - the first data touchpoint (#1). Once Maya's identity is verified, Maya can use Practo's registry of verified doctors to find a gynaecologist and book a teleconsultation appointment – the second data touchpoint (#2). Maya must share her medical records with her

[57] *Digital Personal Data Protection Rules, 2025*.
[58] "Defined under §2(i) of the DPDP Act as "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."
[59] Ministry of Electronics and Information Technology, Electronic Consent Framework, 7. See also, Bhojwani, "The Best Way Forward for Privacy."
[60] NITI Aayog, Data Empowerment And Protection Architecture, 52.
[61] Light, "The Walkthrough Method."

gynaecologist via Practo – the third data touchpoint (#3). Maya must collate all her existing medical records, create digital copies of these records if they are in paper form (which is often the case), and upload these records to the Practo app. These records are then stored on Practo servers.[62] Prior to the teleconsultation, Maya's gynaecologist asks A to provide a blood pressure reading. If Maya has a blood pressure machine, she can obtain a reading herself. If not, Maya has to visit a clinic or a pharmacy a few days before her teleconsultation to obtain a blood pressure reading, and then share this reading with her gynaecologist. After the teleconsultation, Maya's gynaecologist issues a prescription to Maya via the Practo app. Maya must then convey this prescription to a pharmacy to obtain the medicines - the fourth data touchpoint (#4). If the gynaecologist recommends that Maya undergo a diagnostic test like a pap smear, Maya must locate a diagnostic clinic for this service. While Practo maintains a list of partner diagnostic labs, Practo may not have a partner-lab who services Maya' location. The lab may also require access to Maya's medical records – the fifth data touchpoint (#5). For this, Maya must collate all her medical records as she did in #2, and share these medical records with the diagnostic lab. After the test, the diagnostic lab may provide paper-based reports of Maya's test which Maya then needs to digitise and reupload on Practo, to convey these results to her gynaecologist – the sixth data touchpoint (#6). The seventh and final instance of data touchpoint (#7) arises if Maya wants to claim reimbursements of medical expenses from her insurance. At present, insurance companies are not integrated onto Practo. As a result, Maya must collate her prescriptions, test reports and receipts from Practo, and share this data with her insurance company via a separate platform.

What emerges from this walkthrough is the number of times Maya needs to share her medical records among various healthcare actors. The NDHE attempts to 'ease' these data flows. Thus, in the post-NDHE scenario, Maya will be issued an ABHA when she registers on Practo, or if she already has an ABHA, she will create an account on Practo using this ABHA.[63] Thereafter, all of Maya's health records will be linked to her ABHA – including her existing medical records that she digitises and uploads to Practo, as also all the medical records created by her gynaecologist, her pharmacy and her diagnostic lab. And finally, Maya does not have to initiate and manage each set of data transfer on her own. Instead, she can enlist an intermediary, known as a consent manager. Maya will communicate her preferences to the consent manager with regard to the sharing of her data in an electronic format. The consent manager will then ensure that this electronic consent for each data transaction is communicated to the relevant actors, and will arrange for a direct data transfer of Maya's data - for example a direct transfer of Maya's prescription from her gynaecologist to the pharmacy, Maya's lab results from the diagnostic lab to her gynaecologist, and in the future, all of Maya's data to her insurance company, along with an artefact containing the terms of Maya's consent for each instance of data sharing. This consent-based data flow is visualised in Figure 3.

[62] Practo, "Terms and Conditions", §3.10.18
[63] Practo, "ABHA ID."

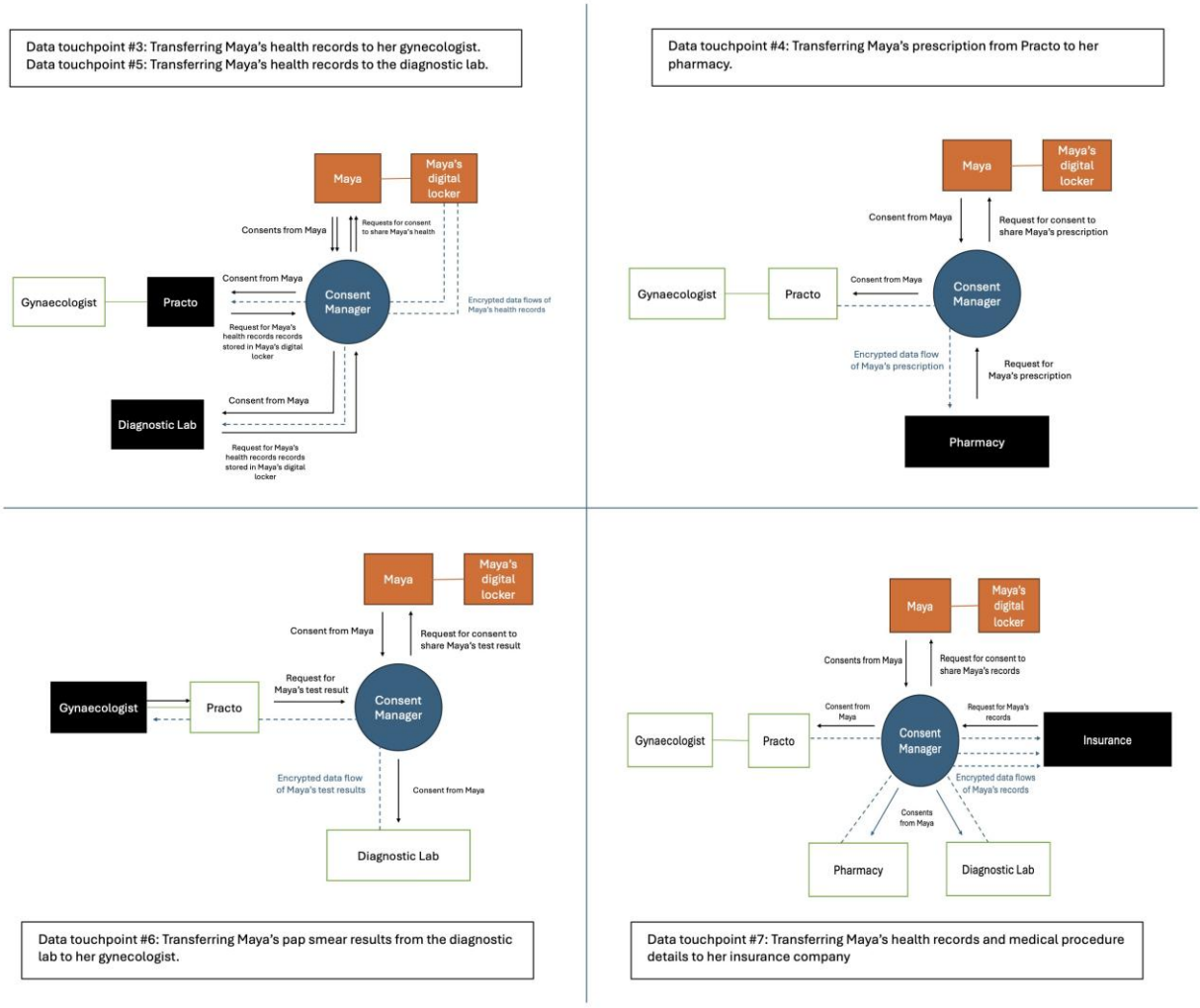


Figure 3. Author's visualisation of consent framework in operation during Maya's walkthrough on Practo

This consent framework can significantly reduce compliance costs for healthcare providers, particularly small and medium enterprises. It also responds to the problem of consent fatigue – where the increasing use of digital platforms and services has resulted in individuals being inundated with consent requests, leading to such individuals mindlessly authorsing these requests as opposed to providing informed consent.[64]

The Consent Framework and Informational Self-Determination

In the landmark *Puttawswamy (Right to Privacy)* case, the Indian Supreme Court recognised that informational self-determination is part of the fundamental right to privacy, and that informed consent is central to its realisation.[65] The court recognised the dual nature of the right to privacy - as a constitutionally protected fundamental right in India in cases of interference by the state or public entity, and as a common law right where interferences are by non-state actors.[66] The court also noted that individuals should be able to control the dissemination of their personal information, as part of their fundamental right to autonomy.[67]

[64] Solove, "Murky Consent."
[65] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, (2017) 10 S.C.R 569; *Distt. Registrar & Collector, Hyderabad & Anr. vs. Canara Bank Etc*., (2005) 1 SCC 496. See also Bhatia, "The Supreme Court's Right to Privacy Judgment – IV."
[66] *Justice K.S.Puttaswamy (Retd) and Anr v. Union of India and Ors*, (2017) 10 S.C.R 569 (per Chandrachud, J., concurring); *Justice K.S.Puttaswamy (Retd) and Anr v. Union of India and Ors*, (2017) 10 S.C.R 569 (per Bobde, J., concurring).
[67] Bhatia, "The Supreme Court's Right to Privacy Judgment – IV."

In a later case dealing with the constitutionality of India's national biometric identity program, the court noted that biometric data amounts to sensitive personal data, and as a result, there must be proper legal provisions for notice, consent, access to biometric data, data minimisation and data security.[68] Justice Chandrachud's dissenting opinion in this case notes that biometric data is intimately connected to individuals, their bodies, and to characteristics that make them 'human.'[69] Accordingly, he goes on to note that '[o]ne way of avoiding unnecessary collection of biometric data is to set *strict* legal standards to ensure that the intrusion into privacy is commensurate with and proportional to the need for the collection of biometric data.'[70] (emphasis added).

When it comes to health data under the NDHE, the legal questions are whether: (i) the fundamental right to privacy applies to the flow of health data within the NDHE, and (ii) if yes, whether the consent framework as under the DPDP Act (combined with other provisions under the DPDP Act) constitutes a reasonable restriction of the right to privacy. From the jurisprudence of the Indian Supreme Court, it is clear that health data flows in the NDHE attract the right to privacy. In the *Puttawswamy (Right to Privacy)* case, Justice Chandrachud specifically referred to a reasonable expectation that people have in wanting to keep sensitive data such as health information or health records private.[71] At the same time, he and other judges acknowledged the public benefits that certain kinds of health data hold, particularly for scientific research, thereby indicating that some health data flows are necessary.

Whether then the consent framework constitutes a reasonable restriction of the right to privacy is more difficult to resolve. To assess this question, the Indian Supreme Court has postulated a three-prong test – whether the restriction is prescribed by law, whether it is necessary to achieve its purpose, and whether it is proportional to this stated purpose.[72] Regarding the first prong on legality, from 2021 when the NDHE project was officially launched and until the DPDP Act comes fully into effect, it can be argued that there is no specific law for authorising health data flows under the NDHE, and the Health Data Management Policy is not a law as it is an executive policy. But perhaps more importantly, are the second on necessity and the third prong on proportionality. For the collection of biometric data under India's Aadhaar program, the Indian Supreme Court recognised that necessity was fulfilled since the collected biometric data was being used to enable access to social welfare entitlements and to plug diversions and leakages.[73] But with the NDHE, a similar argument that health data flows are necessary for enabling access to healthcare and plugging leakages from public insurance schemes may be harder to sustain, due to the market-driven approach to universal health coverage in India combined with the political economy of health data monetisation which shapes the architecture of the NDHE (as discussed in Section II above). And when it comes to the prong of proportionality, it can be argued that the consent framework does not provide meaningful decisional autonomy to individuals, in a context of health data monetisation.

Operationalising Consent for Informational Self-Determination in a Data Market

The consent framework of the DPDP Act (and the Health Data Management Policy) is based on a series of assumptions – *one*, that health data is an object distinct from (the bodies of) individuals who produce it and distinct from various social, computational, economic and legal processes that bring data into existence; *two*, that health data therefore bears commodity-like characteristics; and *three,* individuals should alienate their data through property law and/or specify terms of use for their data through contract law.

When health data is aggregated into datasets or when health data is recorded in material artefacts like medical records and stored on physical artefacts like servers, individuals do exercise some property-like rights, such as the right to access their data, enable others to use their data, or transfer ownership of their datasets. However, there are also some rights that arise not because data is the property of an individual, but because data is an *extension* of individual selfhood.[74] The right to non-discrimination in data-driven decision-making is one such right, recognised by the Indian Supreme Court.[75] In the context of health data, the feminist think tank Internet Democracy Project characterises health data as an *embodied resource* – i.e. as a resource that is not just a computational artefact, but that always contains a 'link between a patient's body and the data generated by it.'[76]

[68] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, 2019 (1) SCC 1 (per J. Sikri and per J. Chandrachud).
[69] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, 2019 (1) SCC 1 (per Chandrachud, J)
[70] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, 2019 (1) SCC 1 (per Chandrachud, J)
[71] *Justice K.S.Puttaswamy (Retd) and Anr v. Union of India and Ors*, (2017) 10 S.C.R 569 (per Chandrachud, J), 774-775.
[72] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, (2017) 10 S.C.R 569.
[73] *Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors*, 2019 (1) SCC 1 (per J. Sikri).
[74] Salome Viljoen refers to this as the 'dignitarian approach' to data governance. For a further discussion on the property-based and dignitarian approaches to data governance, see Viljoen, "A Relational Theory of Data Governance."
[75] *Justice K.S.Puttaswamy (Retd) and Anr v. Union of India and Ors*, (2017) 10 S.C.R 569 (per Chandrachud, J., concurring).
[76] Radhakrishnan, Health Data as Wealth.

While health data is a valuable resource for both individual wellness as well as public goals of science and research, given its inherent link to the body, the commodification of health data no doubt triggers personal and social contestations, and as such, begs the crucial question – under what conditions should health data be commodified? Charlotte Ducuing (drawing from Margaret J Radin) argues that the commodification of data more generally should be approached as a spectrum. From here, the non-commodification end of the spectrum can be operationalised by drawing on a theory of personhood – 'namely one that is not "the self as pure subjectivity standing wholly separate from an environment of pure objectivity," but one that recognises the relationship between personhood and contextuality.'[77] Such an approach allows us to move away from markets as the default institution for alienation of data as under the NDHE, but instead treat market-based data exchange mechanisms as purpose-specific and purpose-bound.

In a similar vein, Julie E. Cohen argues that privacy should be an environmental condition, and consent as a tool for individual as well as collective boundary management when interacting with networked technologies.[78] Daniel J. Solove further argues that consent will never be 'perfect,' but is still necessary for personal data management[79] - a point echoed by the Indian Supreme Court as well.[80] Accordingly, Solove proposes a set of duties that must be performed by entities seeking consent for personal data flows – the duty to obtain consent through appropriate processes, the duty to avoid thwarting reasonable expectations of privacy, the duty of loyalty to place the individual's interest above the entity using personal data, and the duty to avoid unreasonable risk to individuals.[81] Thus, even in situations where data is sought to be regulated as an economic resource and if the exchange of data by individuals is considered welfare-maximising, such exchange could be 'fair' if combined with the obligations specified above and if undertaken with due regard for the capacity of different individuals to exercise informed consent.[82]

Some medical laws prescribe substantive and procedural requirements for informed consent. For example, under the *Human Immunodeficiency Virus And Acquired Immune Deficiency Syndrome (Prevention And Control) Act, 2017,* any testing or treatment for HIV requires informed consent from the patient, and informed consent is defined to mean: (i) consent without any coercion, undue influence, fraud, mistake or misrepresentation, (ii) consent relating to risks and benefits of, and alternatives to, the proposed intervention in such language and in such manner as understood by the patient, (iii) that the patient must bear the capacity to consent, and (iv) that consent is accompanied by pre- and post-testing/treatment counselling.[83] Similar requirements for informed consent in the context of mental health treatments are contained with the *Mental Healthcare Act of 2017*.[84] This law also identifies a set of supported-decision-making tools that can be used by patients.[85] Empirical research reveals that some aspects of these laws, such as post-treatment counselling, are not always operationalised in practice.[86] Nonetheless, the laws themselves are more attuned to consent as socially-situated, and accordingly require entities seeking consent to perform a range of secondary actions to ensure that consent is legitimate.

Shortcomings of the NDHE's Consent Framework

However, the logic underpinning the consent framework - that consent can and should be abstracted from data flows – is based on a *purely* propertarian approach to health data; more specifically, an approach that sees data as a national asset and the Indian market as the default mechanism for realisation of value from this asset. Within this approach, a 'fair' market for exchange/flow of health data (unlike Solove's model) is one that is not monopolised by Big Tech actors, but one where '[a]ccessability of data to Indian actors (companies, individuals, and the government) remains the primary strategic interest of the Indian state.'[87]

[77] Ducuing, Data Commodification and the Law, Ch 2.
[78] Cohen, Between Truth and Power, 67.
[79] Solove, "Murky Consent." See also Taylor, "Protecting Privacy in India."
[80] *Justice K.S.Puttaswamy (Retd) and Anr v. Union of India and Ors*, (2017) 10 S.C.R 569 (per Kaul, J.)
[81] An expert committee was constituted by the Indian Government in 2017 to examine issues related to data protection, recommend methods to address them, and draft a data protection bill. It in its report, this expert committee also recognised that the normative aspect of consent needs to be preserved, by imposing certain fiduciary obligations on data controllers who rely on consent-based data processing. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, A Free and Fair Digital Economy.
[82] See Coll, Personal Data Empowerment; Ducuing, "Data as a Contested Commodity."
[83] *Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Act, 2017*, §2(b), §2(n), §5.
[84] *Mental Healthcare Act, 2017*, §2(i), §86(5).
[85] Kapoor, "Decisional Privacy and Decisional Autonomy."
[86] See, for example, Nataraj, "Consent Is Compulsory."
[87] Mishra, "Data as a National Asset"; Basu, Sovereignty in a 'Datafied' World.

In policy documents, the consent framework is defined as the 'Data Empowerment and Protection Architecture.'[88] But by design, the consent framework valorises a monolithic vision of individual empowerment over health data flows, one where a patient's participation in networked health technologies is always assumed to be necessary and in the best interest of the patient.[89] While the consent framework and the DPDP Act allow for revocation and modification of consent, the ability of a patient to opt out entirely of NDHE health data flows while having at least similar quality of healthcare is limited, in large part because of the surrounding environment of incentives and coercion around the enrolment of patients into the NDHE. For instance, ABHA IDs were issued to individuals without their consent during the COVID-19 pandemic, and later used to create electronic health data records for these individuals.[90] Some states made ABHA mandatory for availing access to government health schemes.[91] Further, to incentivise uptake of the health data standards, the NHA provides a financial incentive to healthcare providers for each electronic health record created using the NDHE specifications.[92] Private actors are therefore incentivised to adopt manipulative design and messaging, to link service delivery to the possession of an ABHA. For example, ICICI Lombard (a popular insurance company) issues detailed instructions on its website for obtaining and using ABHA, and only includes one FAQ at the bottom of the webpage stating that ABHA 'is not mandatory but highly recommended for easy access to healthcare services.'[93] As Avantika Tewari notes, the techno-legal approach of the consent framework transforms 'the user into a consenting data node,' who supplies their health data as the raw material for platformatised healthcare under the NDHE, and in doing so, the consent framework 'empties privacy of its antagonism.'[94]

There are complex tradeoffs between the need to build digital systems to improve patient outcomes and share health data for public good such as disease monitoring and research on the one hand, and the use of health data to create digital health apps by Indian start-ups and companies on the other hand. The consent framework however, recasts consent as a mechanism to reduce transaction costs in the exchange of health data, thereby using consent as a means to reduce 'frictions' in any and all health data flows. As a result, the consent framework does not enable data minimisation, nor serve as a tool for individuals to question whether datafication is necessary *at all,* to engage in digital disengagement and to set the terms of datafication. By integrating this consent framework into the DPDP Act, the legal principle of informed consent becomes what Nayantara Ranganathan describes as 'a mimicry of the direction the market for data takes.'[95] In other words, there is a continuous 'legal coding' of health data as an asset traded by data fiduciaries where the exchange value is determined by commercial actors who effect the health data flows and benefit from it,[96] and the social value derived from health data flows is understood as the potential of health data flows to enable market-led health innovations.

This legal coding entrenches health consumerism through digital health apps as the preferred approach to universal health coverage, as opposed to allowing space for experimentation with other public health or universal health approaches.[97] This also spurs a marketplace of consent managers themselves, where again issues relating to quality and manner of obtaining informed consent will be addressed by market-participants themselves, as opposed to by law.[98]

The Consent Framework Should Instead Embrace Friction

As scholars of Science and Technology Studies note, frictions are social and physical factors such as 'the costs in time, energy, and attention required simply to collect, check, store, move, receive, and access data,' which impede scientific knowledge production.[99] But, there is also a politics to these frictions – in terms of who can assert these frictions, and for what purposes.[100] For instance, Jo Bates writes that '[w]hile data friction may be a frustration to overcome in some cases for some people, in other cases, including those related to online activity, people feel powerless to generate enough friction in relation to the movement of data.'[101]

[88] NITI Aayog, Data Empowerment And Protection Architecture.
[89] Parsheera, "An Analysis of India's New Data Empowerment Architecture."
[90] Rana, "COVID-19 Vaccine Beneficiaries"; Ghosh, "Used Aadhaar for Covid Vaccine? "; Dogra, "Took Covid Vaccine Using Aadhaar?"
[91] Ray, "Mandatory Linking of CGHS Beneficiary ID with ABHA"
[92] National Health Authority, Digital Health Incentive Scheme.
[93] ICICI Lombard, "ABHA Card Benefits, Uses and Registration Explained."
[94] Tewari, "The Politics of Data in India's Platform State."
[95] Ranganathan, "The Economy (and Regulatory Practice) That Biometrics Inspires," 60.
[96] Van Dijck, "Understanding the Promises and Premises of Online Health Platforms"; Pistor, The Code of Capital.
[97] Sekalala, "A Socio-Legal Critique of Digital Health Commercialization in Sub-Saharan Africa."
[98] The NDH Blueprint for instance, refers to the creation of "consent-management-as-a-service", as a benefit of the NDHE. See Ministry of Health and Family Welfare, National Digital Health Blueprint, 23.
[99] Edwards, A Vast Machine, 84.
[100] Bates, "The Politics of Data Friction."
[101] Bates, "The Politics of Data Friction," 418.

Brett M. Frischmann and Evan Selinger argue that modern data-driven technologies constantly extract data from individuals, and the networked society is 're-engineering humanity' to render it more calculable and predictable.[102] Frischmann and Susan Benesch further argue that there is a moral value to friction in the networked society – as a type of resistance necessary for individual decision-making and to form social relations.[103] Legal frameworks must therefore engender friction-in-design in the form of 'politically, technologically, and socially engineered transaction and interaction costs,' as a type of speed bump or 'legal drag' built into the design of digital technologies.[104] Some examples include legal mandates for comprehension checks to test whether people anticipate the possible reach of their digital communications, and design interfaces that require 'active opt-in' for certain kinds of data activities like sharing of geolocation data.[105] I argue that the consent framework for the NDHE should similarly be implemented as a form of friction-in-design regulation.

The Consent Framework as a Form of Friction-In-Design Regulation

Neither the DPDP Act nor the DPDP Rules contain fiduciary obligations as part of the consent framework similar to those proposed by Solove, nor do they prescribe additional decision-support provisions for consent as in other medical laws. These provisions are also absent in regulatory frameworks specific to digital health, such as the *Telemedicine Practice Guidelines*.[106] But instead of treating consent as a mechanism to reduce transaction costs in health data flows, we should consider consent as a mechanism that enables the internalisation of certain externalities. In order to ensure that normative legal principles of informational self-determination are safeguarded, I argue that the consent framework should be operationalised as a framework that introduces a necessary amount to drag in health data flows while still ensuring health data flows at scale.

For instance, in November 2025, the delegated rules to the DPDP Act were published (DPDP Rules), and will come into effect in a phased manner.[107] The DPDP Rules prescribe certain obligations for consent managers – such as the requirement to maintain a website and/or app through which their services can be accessed and effected; and to maintain a record of all consent provided, denied or withdrawn by an individual and the noticed accompanying each request for consent on their website and app.[108] I argue that further obligations on consent managers should be included with regard to the design of their website/app – notably the obligation to carry out regular comprehension checks for consent transactions, and the obligation to display a visual dashboard indicating the total number and types of consent provided by an individual whenever a new consent is sought so that the individual user can easily 'see' their past actions and factor their past decisions into their current deliberation.

The DPDP Rules further specify that an entity wishing to be a consent manager must submit an application to a newly-appointed authority known as the Data Protection Board of India (Board).[109] In evaluating this application, one of the factors the Board must consider is whether 'the applicant has sufficient capacity, including technical, operational and financial capacity, to fulfil its obligations as a Consent Manager.'[110] I argue that an additional clarification should be added here, relating to the capacity of the applicant to engage in user-friendly, participative and/or collaborative design approaches, which can be evaluated by considering, for instance, whether the applicant will have specific posts for website/app design which will be occupied by employees with participative design skills.

I propose that the Board should maintain a repository of best practices for consent management. For instance, a group of researchers in the US developed a multi-modal smartphone-based interface that can be used by researchers to obtain biomedical data from individuals – comprising of standardised icons and structured text to convey notices about data sharing, and a post-consent quiz to check comprehension and voluntariness of the consent that was provided.[111] Examples like this could be included in the best practices repository, to guide design of consent management platforms.

Finally, the DPDP Rules also require each consent manager to publish on their website/platform, the means by which individuals can exercise data rights such as the right to revoke consent, right to access their personal data, and the right to seek modification/deletion of this data.[112] However, as another friction-in-design regulation, I propose that the DPDP Act should

[102] Frischmann and Selinger, Re-Engineering Humanity.
[103] Frischmann and Benesch, "Friction-In-Design Regulation," 388.
[104] Frischmann and Benesch, "Friction-In-Design Regulation," 390. See also Cohen, Configuring The Networked Self.; Goodman, "Digital Fidelity and Friction"; Ohm, "Desirable Inefficiency."
[105] Frischmann and Benesch, 440–445.
[106] Ministry of Health and Family Welfare, Telemedicine Practice Guidelines.
[107] *Digital Personal Data Protection Rules,* 2025.
[108] *Digital Personal Data Protection Rules,* 2025, Rule 4(3) read with Part B of the First Schedule.
[109] *Digital Personal Data Protection Rules,* 2025, Rule 4(1).
[110] *Digital Personal Data Protection Rules,* 2025, Rule 4(2) read with Paragraph 2 of Part A of the First Schedule.
[111] Doerr, "Implementing a Universal Informed Consent Process for the All of Us Research Program."
[112] *Digital Personal Data Protection Rules,* 2025, Rule 14(1).

instead require these details to be disclosed by applicants wishing to be a consent manager, in their application to the Board. The Board should then verify the completeness of the information provided by the consent managers, as well as ease-of-use of their design interfaces to the extent consent managers seek to facilitate the exercise of these data rights, prior to granting approval to launch.

In this way, the consent framework can be used to enable consent-based health data flows at scale, while ensuring informational self-determination.

B. Regulatory artefacts for impact assessments

Friction-in-design regulation should also be used for impact assessments of digital health technologies.

At the outset, it is important to note that in critical scholarship on data law, legally-mandated data protection impact assessments and algorithmic impact assessments have come under criticism for converting legal norms (such as non-discrimination) into consequentialist risk-based analyses.[113] But impact assessments can also make visible and enable organising and advocacy around these harms.[114]

In India, the obligation to perform periodic data protection impact assessments is only imposed on a special class of actors – 'Significant Data Fiduciaries.'[115] They are specifically notified based on the volume and sensitivity of data they process, the risks they pose to rights of individuals, their potential impact on the sovereignty and security of India, their risk to electoral democracy, and their nexus with public order.[116] While no such entities have been notified so far, it is likely that social media and e-commerce platforms will be identified as Significant Data Fiduciaries – given that India has tried to impose additional obligations on such entities in the past,[117] and given the focus on regulation of such entities in other jurisdictions such as the European Union.

But processing of health data per se does not require a data protection impact assessment under the DPDP Act. In fact, a 2018 draft of the DPDP Act contained more detailed provisions on data protection impact assessments. Section 33(1) of this draft required such assessments to be undertaken when an entity seeks to undertake 'large-scale profiling or use of sensitive personal data such as genetic data or biometric data.' Such impact assessments were to be submitted to the data protection authority prior to commencing the data processing activities, and the data protection authority was vested with the power to mandate a cessation of the proposed data processing activities if it believes the activities may cause harm to individuals.[118] But this provision is not included in the current DPDP Act.

On the other hand, the Health Data Management Policy does contain a broadly worded provision on data protection impact assessments. Section 27(3) of this policy requires all data fiduciaries (public and private sector) to undertake a data protection impact assessment in two situation – prior to processing data as part of any 'new technologies' or where data processing carries significant risk of harm to individuals.[119] But these data protection impact assessments are not required to be made public, nor are there any reporting requirements regarding completion of these assessments. Even annual reports released by the NHA are silent on data protection, data security and surveillance risks of the NDHE – opting instead to highlight the rapid (and allegedly voluntary) uptake of NDHE components.[120] This is particularly concerning given continuing data leaks from the NDHE. In June 2023 for instance, news reports brought to attention a Telegram bot that spewed out personal details of individuals, such as their name, Aadhaar numbers and passport numbers, because of a data leak from CoWIN - India's covid-19 vaccine distribution platform.[121] Currently, the Data Security Council of India – a non-profit that routinely advises the Union government on cybersecurity – is undertaking a cybersecurity assessment of the healthcare industry.[122]

---

[113] Van Dijk, "A Risk to a Right?"
[114] Metcalf, "Algorithmic Impact Assessments and Accountability."
[115] *Digital Personal Data Protection Act, 2023*, §10(2)(c)(i).
[116] *Digital Personal Data Protection Act, 2023*, §10(1).
[117] For example, the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* requires social media platforms to grant significant deference to government bodies in the removal of inappropriate content. Some of the rules were held to be unconstitutional by the Bombay High Court – specially a provision that allowed the federal government to set up fact-checking units to monitor misinformation about the government on social media and required social media platforms to take down any such identified misinformation. See *Kunal Kamra v. Union of India*, WP No. 9792 of 2023, decided on September 26, 2024 (Bombay High Court).
[118] *Personal Data Protection Bill, 2018*, §33(5).
[119] National Health Authority, *Health Data Management Policy*, §27(3).
[120] Available here: https://abdm.gov.in/publications.
[121] Xavier, "Explained."
[122] Staff Reporter, "Data Security Council of India, HIMSS Ink MoU for Healthcare Cybersecurity."

Where impact assessments are undertaken for data-driven digital health interventions, they take the form of 'techno-economic assessments.' For instance, one of the components of NDHE is a digital logistics management system for immusation vaccines, known as the Electronic Vaccine Intelligence Network (or eVIN), which comprises of centralised recordkeeping and a real-time vaccine stock dashboard.[123]

In 2018, the Ministry of Health and Family Welfare undertook a 'techno-economic assessment' of eVIN.[124] This assessment discussed structural aspects of the use of digital systems, such as internet connectivity. But it did not engage with questions of how data was generated and subsequently converted into the eVIN dashboard, labour conditions of the data workers behind eVIN, the kinds of public healthcare policy decisions were being made on the basis of the vaccine stock dashboard, whether any personal data was involved, and if there were any data security risks – questions that should be at the core of any impact assessment of data-driven systems. The calculative logics employed in a techno-economic assessment emerge from a conceptualisation of digital health systems as 'products' in a data-driven economy. But for systems like eVIN, that encourage more data-driven decision-making for the allocation of resources to public health, a 'product-based' assessment misses out on the harms that data-driven systems like eVIN may pose to the fundamental rights of patients, healthcare workers, and vulnerable communities.

To the extent public resources are used to develop data-driven infrastructures for social issues (such as the NDHE), a proportionality analysis between the costs and benefits of the NDHE is necessary. To facilitate this analysis, some researchers have suggested a calculative framework based on the theory of public good, designed using multidisciplinary perspectives.[125] The researchers argue that the ideal functionalities of each component of the NDHE and the associated privacy and security risks should be identified at a granular level, on the basis of which a more thorough proportionality analysis can be undertaken to maps the risks and potential harms of the NDHE against its purported benefits. Legal regulations like the DPDP Act should require data fiduciaries like Practo to design and conduct these types of proportionality analyses at regular intervals and disclose the results to the public. This can be considered as another type of friction-in-design regulation, necessary to ensure the continuous health data flows within the NDHE are aligned with informational self-determination.

IV. Conclusion

To summarise, in this article I argue that central to the NDHE is the constant 'flow' of health data, to enable commercial actors to create digital health apps and monetise these data flows. I also argue that the political economy of the NDHE reshapes data law in its image - particularly informed consent for (personal) data flows, and legal mandates for impact assessments of data-driven technologies.

In response, I argue that it is important to conceptualise and implement certain 'friction-in-design regulations,' i.e. legal mandates that engender a certain amount of drag in the generation and circulation of health data within the NDHE. The framework of health data justice discussed in this Special Issue could hold useful insights on how to build as well as regulate digital health infrastructures that centre dignity, participation, and responsible data practices.

Acknowledgement
The author is grateful for feedback from the Special Issue editors, Mila Samdub, Sandra Bärnreuther, Smriti Sharma and Sreya Dutta Chowdhury for feedback on an earlier version of this article.

[123] Ministry of Health and Family Welfare, "Electronic Vaccine Intelligence Network."
[124] Ministry of Health and Family Welfare, Techno-Economic Assessment of eVIN.
[125] Agarwal, "On Health Data Architecture Design."

Bibliography

Agarwal, Prashant, Subodh Sharma, Ambuj Sagar, and Subhashis Banerjee. "On Health Data Architecture Design." In *Private and Confidential: When Public Health and Privacy Meet in India*, edited by Smriti Parsheera. HarperCollins, 2023.

Ashok, Pratiksha. "The Curious Case of Automated Decision-Making in India." *International Cybersecurity Law Review* 4, no 2 (2023): 235–48. https://doi.org/10.1365/s43439-022-00078-3.

Basu, Arindrajit. *Sovereignty in a 'Datafied' World*. Observer Research Foundation, 2021. https://www.orfonline.org/research/sovereignty-in-a-datafied-world.

Bates, Jo. "The Politics of Data Friction." *Journal of Documentation* 74, no 2 (2018): 412–29. https://doi.org/10.1108/JD-05-2017-0080.

Bhatia, Gautam. "The Supreme Court's Right to Privacy Judgment – IV: Privacy, Informational Self-Determination, and the Idea of Consent." *Constitutional Law and Philosophy*, August 30, 2017. https://indconlawphil.wordpress.com/2017/08/30/the-supreme-courts-right-to-privacy-judgment-iv-privacy-informational-self-determination-and-the-idea-of-consent/.

Bhojwani, Tanuj. "The Best Way Forward for Privacy Is to Open up Your Data." ProductNation, August 21, 2017. https://pn.ispirt.in/the-best-way-forward-for-privacy-is-to-open-up-user-data/.

Birch, Kean. "Rethinking Value in the Bio-Economy: Finance, Assetization, and the Management of Value." *Science, Technology, and Human Values* 42, no 3 (2017): 460–90. https://doi.org/10.1177/0162243916661633.

Biswas, Soutik. "Right to Health: The Fight over Who'll Pay Hospital Bills of India's Poor." *BBC*, April 5, 2023. https://www.bbc.com/news/world-asia-india-65159986.

Chakravarthi, Indira. "Digital Health and the National Digital Health Mission - Leveraging 'Universal Health Care' for Technology and Capital?" *RUPE India*, April 10, 2024. https://rupe-india.org/aspects-no-81-82/digital-health-and-the-national-digital-health-mission/.

Chami, Nandini, R Vaishno Bharati, Anushka Mittal, and Ankita Aggarwal. *Data Subjects in the Femtech Matrix: A Feminist Political Economy Analysis of the Global Menstruapps Market*. ITforChange, 2021. https://itforchange.net/sites/default/files/1620/FDJ-Issue-Paper-6-Data-Subjects-In-the-Femtech-Matrix-IT-for-Change.pdf.

Cohen, Julie. *Configuring The Networked Self: Law, Code, And The Play Of Everyday Practice*. Yale University Press, 2012.

Cohen, Julie E. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press, 2019.

Coll, Liz. *Personal Data Empowerment: Time for a Fairer Data Deal?* The National Association of Citizens Advice Bureaux, 2015. https://assets.ctfassets.net/mfz4nbgura3g/31Xl5fPUaXX5Gdnns1G0QZ/6680fe2258718382fc8d2b9aef1ac9d4/Personal_20data_20empowerment_20report.pdf.

Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. Report to Ministry of Electronics and Information Technology, Government of India, 2018. https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf.

Das, Sohini. "Healthcare Budget 2025: Healthcare Gets 9.78% Boost, Cancer Treatment Costs to Drop." *Business Standard*, February 1, 2025. https://www.business-standard.com/budget/news/budget-2025-healthcare-gets-9-78-boost-cancer-treatment-costs-to-drop-125020101528_1.html.

Dencik, Lina, and Anne Kaun. "Datafication and the Welfare State." *Global Perspectives* 11, no 1 (2020): 12912. https://doi.org/10.1525/gp.2020.12912.

Doerr, Megan, Shira Grayson, Sarah Moore, Christine Suver, John Wilbanks and Jennifer Wagner. "Implementing a Universal Informed Consent Process for the All of Us Research Program." *Pacific Symposium on Biocomputing. Pacific Symposium on Biocomputing* 24 (2019): 427–38.

Dogra, Sarthak. "Took Covid Vaccine Using Aadhaar? Your National Health ID Has Been Created without Your Permission." *India Today*, May 24, 2021. https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24.

Ducuing, Charlotte. "Data as a Contested Commodity." *Global Jurist* 24, no 3 (2024): 277–319. https://doi.org/10.1515/gj-2024-0065.

Ducuing, Charlotte. *Data Commodification and the Law: Navigating Data Markets and Data Protection*. 1st ed. KU Leuven Centre for IT and IP Law. Intersentia, 2025.

Edwards, Paul. *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*. MIT Press, 2010.

Fisher, Angelina and Thomas Streinz. "Confronting Data Inequality." *Columbia Journal of Transnational Law* 60, no 3 (2022): 829–956.
Fourcade, Marion and Kieran Healy. "Seeing like a Market." *Socio-Economic Review*, December 23, 2016, mww033. https://doi.org/10.1093/ser/mww033.
Frischmann, Brett M. and Susan Benesch. "Friction-In-Design Regulation as 21st Century Time, Place, and Manner Restriction." *Yale Journal of Law and Technology* 25, no 2 (2023): 377-447. https://doi.org/10.2139/ssrn.4178647.
Frischmann, Brett and Evan Selinger. *Re-Engineering Humanity*. Cambridge University Press, 2018. https://doi.org/10.1017/9781316544846.
Ghosh, Abantika. "Used Aadhaar for Covid Vaccine? Modi Govt Created Your Digital Health ID without Asking You." *The Print*, October 1, 2021. https://theprint.in/health/used-aadhaar-for-covid-vaccine-modi-govt-created-your-digital-health-id-without-asking-you/742958/.
Ghosh, Parijat, Aarthi Rao, Charles-Antoine Janssen, Ajay Mahipal, and Pinak Shrikhande. *Healthcare Innovation in India*. Bain & Company, 2024. https://www.bain.com/insights/healthcare-innovation-in-india/.
Goodman, Ellen. "Digital Fidelity and Friction." *Nevada Law Journal* 21, no 2 (2021): 623-653.
Gopal, K S Uplabdh. "Union Budget 2025: A Pulse Check on Healthcare." *Observer Research Foundation*, February 4, 2025. https://www.orfonline.org/expert-speak/union-budget-2025-a-pulse-check-on-healthcare.
Hunter, Benjamin M., Susan F. Murray, Shweta Marathe and Indira Chakravarthi. "Decentred Regulation: The Case of Private Healthcare in India." *World Development* 155 (July 2022): 105889. https://doi.org/10.1016/j.worlddev.2022.105889.
ICICI Lombard. "ABHA Card Benefits, Uses & Registration Explained." April 25, 2025. https://www.icicilombard.com/blogs/health-insurance/hi/abha-card-benefits-uses-registration.
Jain, Anushka. "AWS Suggests Changes to Unified Health Interface and Other Building Blocks of NDHM." *MEDIANAMA*, September 8, 2021. https://www.medianama.com/2021/09/223-aws-response-uhi-consultation-2/.
Jain, Anushka. "What Did FICCI, IAMAI, NASSCOM, and CII Say about the Unified Health Interface?" *MEDIANAMA*, September 15, 2021. https://www.medianama.com/2021/09/223-industry-bodies-response-uhi-consultation-3/.
Jain, Dipika. "Regulation of Digital Healthcare in India: Ethical and Legal Challenges." *Healthcare* 11, no 6 (2023): 911. https://doi.org/10.3390/healthcare11060911.
Kanwar, Shiva and Mayank Manish. *Evolution of India's Data Protection Law: A Primer*. Indian Council for Research on International Economic Relations, 2023. https://icrier.org/pdf/IPCIDE-Policy_Brief_4.pdf.
Kapoor, Arjun. "Decisional Privacy and Decisional Autonomy: A Rights-Based Paradigm for Mental Healthcare in India." In *Private and Confidential: When Public Health and Privacy Meet in India*, edited by Smriti Parsheera. HarperCollins, 2023.
Light, Ben, Jean Burgess and Stefanie Duguay. "The Walkthrough Method: An Approach to the Study of Apps." *New Media and Society* 20, no 3 (2018): 881–900. https://doi.org/10.1177/1461444816675438.
Mariwala, Vaibhav and Nikita Kwatra. "What Mandaviya and Vaishnaw Must Do." *The Financial Express*, August 27, 2021. https://www.financialexpress.com/opinion/what-mandaviya-and-vaishnaw-must-do/2318598/.
Metcalf, Jacob, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh and Madeleine Clare Elish. "Algorithmic Impact Assessments and Accountability: The Co-Construction of Impacts." *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, March 3, 2021, 735–46. https://doi.org/10.1145/3442188.3445935.
Ministry of Electronics and Information Technology. *Electronic Consent Framework*. Government of India, 2017. https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf.
Ministry of Electronics and Information Technology, "Notification, G.S.R. 843(E)" (Issued on November 13, 2025). https://egazette.gov.in/WriteReadData/2025/267647.pdf.
Ministry of Health and Family Welfare. "Arogya Manthan 2023 to Mark 5 Years of Ayushman Bharat PM-JAY and 2 Years of Ayushman Bharat Digital Mission." Press Information Bureau, September 24, 2023. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1960140.
Ministry of Health and Family Welfare. "Electronic Vaccine Intelligence Network (eVIN) has ensured essential immunization services during the COVID pandemic." Press Information Bureau, August 3, 2020. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1643172.
Ministry of Health and Family Welfare. *National Digital Health Blueprint, 2020*. Government of India, 2020. https://web.archive.org/web/20251223123100/https://abdm.gov.in:8081/uploads/ndhb_1_56ec695bc8.pdf.
Ministry of Health and Family Welfare. *National Health Policy, 2017*. Government of India, 2017. https://mohfw.gov.in/sites/default/files/9147562941489753121.pdf.
Ministry of Health and Family Welfare. *Techno-Economic Assessment of Electronic Vaccine Intelligence Network*. Government of India, 2018. https://www.undp.org/india/publications/evin-techno-economic-assessment.
Ministry of Health and Family Welfare, *Telemedicine Practice Guidelines: Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine*. Government of India, 2020.

Ministry of Health and Family Welfare. "Update on Ayushman Bharat Digital Mission." Press Information Bureau. December 6, 2024. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2081482.
Mishra, Kushang. "Data as a National Asset: What Does Seeing Data in Terms of an Asset Reveal about Postcolonial State in India?" *Technology and Regulation* 2024 (March 2024): 93–102. https://doi.org/10.71265/1tde8k58.
Mishra, Paro, Ravinder Kaur, Shambhawi Vikram and Prashastika Sharma. "Femtech Apps and Quantification of the Reproductive Body in India: Issues and Concerns." *Current Sociology* 72, no 7 (2024): 1340–59. https://doi.org/10.1177/00113921231206491.
Mishra, Udaya Shankar, Suryakant Yadav and William Joe. "The Ayushman Bharat Digital Mission of India: An Assessment." *Health Systems and Reform* 10, no 2 (2024): 2392290. https://doi.org/10.1080/23288604.2024.2392290.
Nataraj, Shyamala. "Consent Is Compulsory: Informed Consent in HIV Testing of Pregnant Women in India." Monash University, 2011. https://scholar.archive.org/work/w5n76fpozbgvlkjxggw27lzmpi/access/wayback/https://au-east.erc.monash.edu.au/fpfiles/16448732/4597654_monash_85461.pdf.
National Health Authority. *Consultation Paper on Operationalising Unified Health Interface (UHI) in India*. Ministry of Health and Family Welfare, 2022. https://web.archive.org/web/20250310005900/https://abdm.gov.in:8081/uploads/Consultation_Paper_on_Operationalising_Unified_Health_Interface_UHI_in_India_9b3a517a22.pdf.
National Health Authority. *Consultation Paper on Unified Health Interface*. Ministry of Health and Family Welfare, 2021. https://web.archive.org/web/20250920041102/https://abdm.gov.in:8081/uploads/UHI_Consultation_Paper_60a9201c1d.pdf.
National Health Authority. *Digital Health Incentive Scheme*. Ministry of Health and Family Welfare, 2023. https://web.archive.org/web/20250908211018/https://abdm.gov.in:8081/uploads/Digital_Health_Incentive_Scheme_3c3766a182.pdf.
National Health Authority. *Health Data Management Policy*. National Health Authority, 2020. https://web.archive.org/web/20250908114115/https://abdm.gov.in:8081/uploads/health_data_management_policy_455613409c.pdf.
National Health Authority. *REQUEST FOR EMPANELMENT: "Selection of Agencies for Providing Fraud Analytics Services for National Health Authority."* RFE Ref. Number: S-12016/41/2021-NHA. Government of India, 2025. https://web.archive.org/web/20250804102617/https://nha.gov.in/img/pmjay-files/RFE_fraud_Analytics_Services.pdf.
National Resource Centre for EHR Standards. "EHR Standards for India." Accessed March 3, 2025. https://www.nrces.in/standards/ehr-standards-for-india#introduction.
National Resource Centre for EHR Standards. "FHIR Implementation Guide for ABDM v6.0.0." January 24, 2024. https://nrces.in/ndhm/fhir/r4/6.0.0/.
NITI Aayog. *National Health Stack: Strategy and Approach*. Government of India, 2018. https://web.archive.org/web/20250207001600/https://abdm.gov.in:8081/uploads/NHS_Strategy_and_Approach_1_89e2dd8f87.pdf
NITI Aayog. *Data Empowerment and Protection Architecture: A Secure Consent-Based Data Sharing Framework to Accelerate Financial Inclusion*. Government of India, 2020. https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf.
Ohm, Paul, and Jonathan Frankle. "Desirable Inefficiency." *Florida Law Review* 70, no 4 (2019): 777-838.
Pandey, Jyoti. *India Stack: Public-Private Roads to Data Sovereignity*. Internet Governance Project, Georgetown University, 2023. https://www.internetgovernance.org/wp-content/uploads/India_stack_9_1_2023.pdf.
Parsheera, Smriti. "An Analysis of India's New Data Empowerment Architecture." In *Emerging Trends in Data Governance*, edited by Swati Punia, Shashank Mohan, Jhalak Kakkar and Vrinda Bhandari. National Law University Delhi Press, 2022. https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-edited-volume-emerging-trends-in-data-governance-343.pdf.
Parsheera, Smriti, ed. *Private and Confidential: When Public Health and Privacy Meet in India*. HarperCollins, 2023.
Pistor, Katharina. *The Code of Capital*. Princeton University Press, 2019.
Practo. "ABHA ID: Your Passport in the Era of Digital Healthcare!" *Practo Digest*, November 7, 2023. https://blog.practo.com/abha-id-your-passport-in-the-era-of-digital-healthcare/.
Practo. "Practo Joins the Ayushman Bharat Digital Mission (ABDM) Ecosystem, with Practice Management Software, Ray." *Practo Digest*, May 2, 2023. https://blog.practo.com/practo-joins-abdm-ecosystem-with-ray-press-release-practo/.
Practo. "Privacy Policy." Practo. Accessed August 21, 2025. https://www.practo.com.
Practo. "Terms and Conditions." Practo. Accessed August 21, 2025. https://www.practo.com.
"Practo Reach- A Sponsored Ad Slot for Clinics." Accessed March 5, 2025. https://www.practo.com/providers/clinics/reach.
Qadeer, Imrana, K. B. Saxena and P. M. Arathi, eds. *Universalising Healthcare in India: From Care to Coverage*. Springer, 2021. https://doi.org/10.1007/978-981-16-5872-3.
Radhakrishnan, Radhika. *Health Data as Wealth: Understanding Patient Rights in India within a Digital Ecosystem*. Internet Democracy Project, 2021. https://internetdemocracy.in/reports/health-data-as-wealth.

Radhakrishnan, Radhika. "Safeguarding Patient Rights under the National Digital Health Mission through a Feminist Framework of Embodiment." *NLUD Journal of Legal Studies* 3 (2021): 73-88.
Raghu, Archita. "Tamil Nadu's Anganwadi Workers Are Drowning in Data Duties. Apps, OTPs & Digital Surveillance." *ThePrint*, May 19, 2025. https://theprint.in/ground-reports/tamil-nadus-anganwadi-workers-are-drowning-in-data-duties-apps-otps-digital-surveillance/2630552/.
Rana, Chahat. "COVID-19 Vaccine Beneficiaries Were Assigned Unique Health IDs without Their Consent." *The Caravan*, October 1, 2021. https://caravanmagazine.in/health/covid-19-vaccine-beneficiaries-were-assigned-unique-health-ids-without-their-consent.
Ranganathan, Nayantara. "The Economy (and Regulatory Practice) That Biometrics Inspires: A Study of the Aadhaar Project." In *Regulating Biometics: Global Approaches and Urgent Questions*, edited by Amba Kak. AI Now Institute, 2020. https://iatranshumanisme.com/wp-content/uploads/2020/09/Regulating-Biometrics-Global-approaches-and-urgent-questions.pdf.
Ray, Anulekha. "Mandatory Linking of CGHS Beneficiary ID with ABHA for Central Govt Employees Suspended; Should You Still Do It?" *The Economic Times*, June 27, 2024. https://economictimes.indiatimes.com/wealth/save/mandatory-linking-of-cghs-beneficiary-id-with-abha-for-central-govt-employees-suspended-should-you-still-do-it/articleshow/111309492.cms?from=mdr.
Sadowski, Jathan. "When Data Is Capital: Datafication, Accumulation, and Extraction." *Big Data and Society* 6, no 1 (2019): 2053951718820549. https://doi.org/10.1177/2053951718820549.
Samdub, Mila. *"Digital Public Infrastructure" at a Turning Point*. Open Future, 2025. https://openfuture.eu/wp-content/uploads/2025/03/250224_DPIAtATurningPoint.pdf.
Samdub, Mila T. "The State and Software Capital." *Phenomenal World*, October 16, 2025. https://www.phenomenalworld.org/analysis/digital-india/.
Sarwal, Rakesh, Urvashi Prasad, K. Madan Gopal, et al. *Investment Opportunities in India's Healthcare Sector*. NITI Aayog, 2021. https://www.niti.gov.in/sites/default/files/2023-02/InvestmentOpportunities_HealthcareSector.pdf.
Schäferling, Stefan. *Governmental Automated Decision-Making and Human Rights: Reconciling Law and Intelligent Systems*. Vol. 62. Law, Governance and Technology Series. Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-48125-3.
Sekalala, Sharifah, and Tatenda Chatikobo. "Colonialism in the New Digital Health Agenda." *BMJ Global Health* 9, no 2 (2024): e014131. https://doi.org/10.1136/bmjgh-2023-014131.
Sekalala, Sharifah, Belinda Rawson, and Pamela Andanda. "A Socio-Legal Critique of the Commercialization of Digital Health in Sub-Saharan Africa." *Policy Studies* 47 vol 2 (2026): 285-305. https://doi.org/10.1080/01442872.2025.2451966.
Solove, Daniel J. "Murky Consent: An Approach to the Fictions of Consent in Privacy Law." *Boston University Law Review* 104 (2023): 593-639. https://doi.org/10.2139/ssrn.4333743.
Staff Reporter. "Data Security Council of India, HIMSS Ink MoU for Healthcare Cybersecurity." Healthcare Asia Magazine, May 2, 2025. https://healthcareasiamagazine.com/healthcare/news/data-security-council-india-himss-ink-mou-healthcare-cybersecurity.
Taylor, Mark J, and Jeannie Marie Paterson. "Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection." *Indian Journal of Law and Technology* 16, no 1 (2020): 71-102.
Tewari, Avantika. "The Politics of Data in India's Platform State." *Economic and Political Weekly* 60, no 51 (2025). https://www.epw.in/journal/2025/51/commentary/opacity-design.html.
Thaker, Aria. "The New Oil: Aadhaar's Mixing of Public Risk and Private Profit." *Caravan*, May 1, 2018. https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit.
Upadhaya, Sayantani. "Why The Digital Dream Soured Quickly For Anganwadi Workers." *BehanBox*, December 20, 2023. https://behanbox.com/2023/12/20/why-the-digital-dream-soured-quickly-for-anganwadi-workers/.
Van Dijck, José, and Thomas Poell. "Understanding the Promises and Premises of Online Health Platforms." *Big Data and Society* 3, no 1 (2016): 2053951716654173. https://doi.org/10.1177/2053951716654173.
Van Dijk, Niels, Raphaël Gellert, and Kjetil Rommetveit. "A Risk to a Right? Beyond Data Protection Risk Assessments." *Computer Law and Security Review* 32, no 2 (2016): 286–306. https://doi.org/10.1016/j.clsr.2015.12.017.
Viljoen, Salomé. "A Relational Theory of Data Governance." *The Yale Law Journal* 31, 2021. https://yalelawjournal.org/feature/a-relational-theory-of-data-governance.
Xavier, John. "Explained: What Does the Alleged CoWIN Data Leak Reveal?" *The Hindu*, June 17, 2023. https://www.thehindu.com/sci-tech/technology/explained-what-does-the-alleged-cowin-data-leak-reveal/article66980831.ece.

Legal Sources

Digital Personal Data Protection Act, 2023 (Ind).
Digital Personal Data Protection Rules, 2025 (Ind).

Distt. Registrar & Collector, Hyderabad And Anr. vs Canara Bank Etc., (2005) 1 SCC 496.
Draft Digital Information Security in Healthcare Bill, 2018 (Ind).
Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Act, 2017 (Ind).
Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Ind).
Justice K.S.Puttaswamy(Retd) And Anr. vs. Union Of India And Ors, (2017) 10 S.C.R 569.
Justice K.S.Puttaswamy(Retd) And Anr. vs. Union Of India And Ors, (2019) 1 SCC 1.
Mental Healthcare Act, 2017 (Ind).
Personal Data Protection Bill, 2018 (Ind).
Syndicate Bank vs. Ramachandran Pillai and Ors., (2011) 15 SCC 398