API ACCOUNTABILITY IN INDIA'S HEALTH DATA INTEROPERABILITY ECOSYSTEM: A DOCTRINAL LEGAL ANALYSIS OF THE ABDM FRAMEWORK

Manika Sharma, NLU Jodhpur

ABSTRACT

The Ayushman Bharat Digital Mission ('ABDM') by India has created an ecosystem involving hospitals, laboratories, insurance providers, and third-party apps using the health data exchange protocol based on Application Programming Interface ('API') and the Fast Healthcare Interoperable Resources (FHIR) standards. However, even though there is a robust mechanism to facilitate the interoperability of health data, the legal rules governing the attribution of accountability concerning such data exchanges via APIs is still far from clear. This article conducts a doctrinal analysis of accountability in API-based data exchanges in the context of ABDM using the right to privacy as derived from Justice K.S. Puttaswamy v. Union of India, the Digital Personal Data Protection Act 2023 (DPDP Act), Information Technology Act 2000 (IT Act), and the Consumer Protection Act 2019 (CPA). Specifically, it shows that the lack of a functional distinction between the categories of 'data fiduciary' and 'data processor' recognized in the DPDP Act leads to a classificatory deficit in respect of 'API intermediaries,' which controls conditions of transfer but not its purposes. The article proposes a 'layered API accountability' framework recognizing the API intermediary as a new legal category, deriving three operational principles: proportional liability, purpose-bound granular consent, and mandatory security-by-design anchored to ISO 27799:2025 and the NIST Cybersecurity Framework.

Keywords: API accountability; health data interoperability; ABDM; DPDP Act 2023; API intermediary.

I. Introduction

The digitalization of healthcare systems globally has been characterized by a shift from proprietary data exchange mechanisms toward open, standards-based Application Programming Interfaces ('APIs').[1] In India, this transformation is anchored in the Ayushman Bharat Digital Mission ('ABDM'), the initiative for unified digital healthcare ecosystem. The ABDM originated as the National Digital Health Mission (NDHM), and launched nationally on September 27, 2021.[2] Its architecture is deliberately API-centric: the Health Information Exchange and Consent Manager ('HIE-CM') relies on FHIR-compliant APIs to facilitate the creation, retrieval, and transfer of patient records across hospitals, clinics, laboratories, pharmacies, insurers, and third-party applications.[3]

Despite all its architectural complexity, an important accountability gap still exists. The uncertainty regarding the accountability allocation for the accuracy, security, and compliance with data privacy policies arises when health data undergoes multiple chained API transactions from the hospital's EHR system through the Consent Manager to the insurer's claims management platform, further to another third-party wellness app.[4] The governance of the API-mediated transactional chain in question is distributed across the DPDP Act,[5] IT Act,[6] the Health Data Management Policy ('HDMP'),[7] combination of other specialized policy documents that lack the needed accountability framework for the transaction at hand.[8] As shown empirically by the studies, the consent mechanisms for health data in the digital space of India are far from being sufficient for such a complicated and technically complex transaction as API-mediated health data sharing.[9]

---

[1] HL7 INT'L, *Overview – Architects*, FHIR SPECIFICATION (v5.0.0: R5) (2023), https://hl7.org/fhir/overview-arch.html.

[2] MINISTRY OF HEALTH & FAMILY WELFARE, GOV'T OF INDIA, NATIONAL DIGITAL HEALTH BLUEPRINT (2019), https://abdm.gov.in/strapicms/uploads/ndhb_1_56ec695bc8.pdf.

[3] NAT'L HEALTH AUTH., NATIONAL DIGITAL HEALTH MISSION: STRATEGY OVERVIEW (2020), https://abdm.gov.in/strapicms/uploads/ndhm_strategy_overview_1aebd4820e.pdf.

[4] Prashila Dullabh et al., *Application Programming Interfaces in Health Care: Findings from a Current-State Sociotechnical Assessment*, 11 APPLIED CLINICAL INFORMATICS 59, 65–66 (2020).

[5] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [*hereinafter* DPDP Act].

[6] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [*hereinafter* IT Act]. Section 43A and the SPDI Rules remain in force until May 13, 2027, pursuant to DPDP Act § 44(2); Gazette Notification No. G.S.R. 846(E) (Nov. 13, 2025).

[7] NAT'L HEALTH AUTH., NDHM HEALTH DATA MANAGEMENT POLICY (2020) [*hereinafter* HDMP], https://abdmbeta.abdm.gov.in/strapicms/uploads/health_management_policy_bac9429a79.pdf.

[8] Shefali Malhotra et al., *Analysing the NDHM Health Data Management Policy* (Ctr. for Health Equity, L. & Pol'y, Working Paper, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947598.

[9] Nivedita Saksena et al., *Rebooting Consent in the Digital Age: A Governance Framework for Health Data*

The two major questions addressed in this paper are as follows. First, how well does the current legal framework allocate accountability in health data interoperability among a number of actors? Second, how can this problem be solved from a doctrinal standpoint?

Key contributions of the paper can be highlighted into two categories: one being the identification of a basic classification gap in the DPDP Act where the distinction between 'fiduciary' and 'processors' overlooks the key role played by the 'API intermediary' in the functioning of the ABDM; and two, the introduction of the 'layered API accountability model' comprising three guiding principles: proportional liability, purpose-bound granular consent, and security by design anchored to international standards including ISO 27799:2025. The analysis engages comparatively with the European Health Data Space ('EHDS') Regulation and the United States interoperability framework under the 21st Century Cures Act.

This research proceeds as follows. Part II describes the ABDM API ecosystem and its five actor categories. Part III maps the existing legal framework, including the constitutional foundations, the DPDP Act's limitations, and the critical transitional regime. Part IV identifies four accountability gaps, centred on the novel claim that the DPDP Act's classificatory binary is the root cause of the deficit. Part V provides comparative insights from both EU and US models. Part VI outlines the proposal for the API Accountability Framework, along with a sample statute. Part VII presents the conclusions drawn.

II. The ABDM API Ecosystem

The ABDM framework is built on a federated system where the health records stay where they were created in hospitals, laboratories, and clinics, and are only exchanged using APIs once the consent from the data owner is received.[10] The system purposefully does not centralize health records into one place but uses a series of APIs for real-time access to the data.[11] The technology that powers the infrastructure above is FHIR[12], which is an international standard specification that is managed by HL7 International[13]. This standard defines granular and

Exchange, 6 BMJ GLOB. HEALTH e005057 (2021).
[10] NAT'L HEALTH AUTH., MINISTRY OF HEALTH & FAMILY WELFARE, GOV'T OF INDIA, DRAFT HEALTH DATA MANAGEMENT POLICY (ABDM) (Version 2, Apr. 2022).
[11] Subrahmanyasarma Chitta et al., *Unlocking Health Data: API-Driven Solutions for Interoperability Challenges*, 2 J. INFORMATICS EDUC. & RSCH., no. 3, 2022.
[12] Nan Hong et al., *Integrating Structured and Unstructured EHR Data Using an FHIR-based Type System: A Case Study with Medication Data*, 2017 AMIA JT. SUMMITS TRANSLATIONAL SCI. PROC. 74 (2018).
[13] Joshua C. Mandel et al., *SMART on FHIR: A Standards-Based, Interoperable Apps Platform for Electronic Health Records*, 23 J. AM. MED. INFORMATICS ASS'N 899 (2016).

resource-based APIs for health data.[14] FHIR divides the health care data into smaller units known as 'Resources' including Patient, Observation, DiagnosticReport, MedicationStatement, AllergyIntolerance, Condition, and over 140 other resources that are available through the RESTful API. Not only does this level of granularity provide the foundation for successful interoperability, but it also creates a major issue of responsibility as the access via API gives access to personal health data at a granularity that cannot possibly be understood or even agreed upon by patients.[15].

There are five separate types of actors involved in the ABDM system. Health Information Providers (HIPs), including hospitals, clinics, diagnostic labs, and pharmacies, create health information and make it accessible via FHIR-based APIs. Health Information Users (HIUs), such as doctors who need the patient's medical history and insurance companies that process claims or authorized researchers working on a project, access the data via API calls.[16] Third-party application developers build applications accessing ABDM APIs through sandbox-approved integrations, ranging from wellness tracking to insurance underwriting.[17] The National Health Authority ('NHA') functions as the ecosystem regulator and infrastructure operator.

An ordinary ABDM transaction follows five phases, namely: (i) creation/updating of ABHA by the individual along with linking of records from participating HIPs; (ii) initiation of data request by the HIU, indicating patient, data types, purpose of use, and duration of use; (iii) presentation of the data request by the Consent Manager to the individual, after which the individual consents or denies permission; (iv) on obtaining consent, the Consent Manager sends signed consent artifact to the HIP, which then encrypts the requested data and sends it via Gateway to the HIU; and (v) decryption and processing of data by the HIU for the purpose of consent. Each phase raises its own accountability issues. Who is responsible if there is an error in record generation, data corruption, inappropriate data access, and excessive retention of data?

---

[14] Bhavani Pasumarthi & Deepro Guha, *Ayushman Bharat Digital Mission: India's Healthcare ODE*, THE QUANTUM HUB (Aug. 2022), https://thequantumhub.com/wp-content/uploads/2022/09/Ayushman-Bharat-Digital-Mission-Indias-Healthcare-ODE.pdf.

[15] M.L. Braunstein, *Health Care in the Age of Interoperability Part 6: The Future of FHIR*, 10 IEEE PULSE 25 (2019).

[16] NAT'L HEALTH AUTH., ABDM HIE-CM CONSENT MANAGER API SPECIFICATION V.3.0 (2024) [*hereinafter* ABDM HIE-CM SPECIFICATION]. The consent artefact operates at the HI-Type (document-bundle) level, not at the individual FHIR resource level.

[17] NAT'L HEALTH AUTH., ABDM SANDBOX GUIDELINES (2022), https://sandbox.abdm.gov.in/.

III. The Existing Legal Framework

A. Constitutional Foundations

The constitutional underpinning has been set out in the landmark decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[18] which determined that there was a fundamental right to privacy under Articles 14, 19, and 21 of the Indian Constitution which constitutes the 'Golden Triangle'. In his judgement, Justice Chandrachud laid down the fourfold criteria to be considered while placing limitations on the right to privacy - legality (based on law), legitimacy (for legitimate state purposes), proportionality (in relation to the object sought), and procedural safeguards.[19]

Subsequently, in the case of Aadhaar,[20] the above criteria were expanded with regards to digital data and identification.[21] This proportionality principle carries direct implications[22] for API-mediated health data exchange: if an API endpoint enables access to a broader set of health records than necessary for the consented purpose, the resulting data collection may fail the constitutional proportionality standard even if formal consent has been obtained. The *Puttaswamy* framework thus establishes a constitutional floor below which no statutory or regulatory instrument governing health data APIs may fall.

B. The DPDP Act 2023

The DPDP Act establishes a framework of 'data fiduciary' responsibilities that apply to anyone who decides how Personal Information is processed and for what purposes.[23] According to the Act, Personal Information can only be handled for lawful purpose, and when consent is required, it must be 'freely given, specific, informed, unconditional, and clear.[24] Data fiduciaries must provide itemized notice before seeking consent,[25] implement reasonable security safeguards,[26] and ensure data accuracy and purpose limitation.[27] In the context of the

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[19] *Id.* ¶¶ 26–46 (Chandrachud, J.).
[20] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (India) (Aadhaar judgment).
[21] *Id.* ¶ 447 (Sikri, J.).
[22] COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (Ministry of Elecs. & Info. Tech., Gov't of India 2018).
[23] DPDP Act §§ 2(5), 2(6), 2(17).
[24] DPDP Act § 4(2).
[25] DPDP Act § 5(1).
[26] DPDP Act § 8(4).
[27] DPDP Act § 8(1)–(3).

ABDM ecosystem, any HIP, HIU, or third-party application developer responsible for deciding how health data is processed is considered a 'data fiduciary' as per the DPDP Act. Nonetheless, the general framework of the Act presents three major gaps when it comes to API-facilitated health data interoperability.

First, the Act does not define rules for allocating liability among multiple data fiduciaries involved in a single chained API transaction a scenario fundamental to the ABDM architecture. In a situation where HIP, the Consent Manager, HIU, and the Claims Processing Application all engage in the same data flow, each entity acts as an independent data fiduciary, although there is no clause that deals with their joint responsibility for any harm that occurs at uncertain stages of the process.[28] Second, the consent framework, while requiring specificity and informed agreement, does not address the technical disconnect[29] between the granularity of API-enabled data extraction and the practical comprehensibility of consent requests to patients.[30] The ABDM's consent artefacts specify entity-level and category-level permissions, but the underlying FHIR APIs retrieve data at resource-level granularity far exceeding these categories. Thirdly, the Act's approach to ensuring compliance is geared towards individual data fiduciaries through fines imposed by the Board, rather than addressing interoperable ecosystems of potentially dozens or hundreds of stakeholders.[31]

On 13th November, 2025, the MeitY issued the DPDP Rules, 2025, putting flesh on the bones of the framework laid down in the Act.[32] But in no way do the Rules fill up the structural deficits highlighted in this paper. There is a phased implementation over three phases. Phase 1, starting November 2025, will cover registration of consent managers and Significant Data Fiduciaries. Phase 2, starting November 2026, will cover operational requirements of security and breach notifications. Phase 3, starting May 2027, corresponds to the exclusion of section 43A of the Information Technology Act, 2000 and the SPDI Rules, 2011. One must remember the divide at play in this paper. One camp is the purpose limitation camp which views DPDPA through sections 4, 6, and 7 of the Act. Another camp is the consent manager camp which looks

[28] Isaac S. Kohane, *Ten Things We Have to Do to Achieve Precision Medicine*, 2 NPJ DIGIT. MED. 1 (2019), https://www.nature.com/articles/s41746-019-0158-7.
[29] CONSUMER UNITY & TRUST SOCIETY (CUTS), COMMENTS FOR NATIONAL HEALTH AUTHORITY ON UNIFIED HEALTH INTERFACE CONSULTATION PAPER (2021).
[30] Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 69 (2011).
[31] Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* 18–22 (Carnegie India, Working Paper, 2020).
[32] Digital Personal Data Protection Rules, 2025, Gazette Notification No. G.S.R. 846(E) (Nov. 13, 2025) (India) [*hereinafter* DPDP Rules]. Three-phase implementation: Phase 1 (Nov. 2025), Phase 2 (Nov. 2026), Phase 3 (May 2027).

upon sections 5 to 8 as a delegated fiduciary structure, borrowed from the account aggregator model. The other view, taken by this paper, is of API as the second category. This paper argues that the determination of purposes of processing, as envisaged by sections 4 and 6, cannot be done simply through specifying and publishing a machine readable interface. Rule 6 of the 2025 Rules is of little use in addressing any of the above camps in precise terms. Rather, it sets out general security safeguards for the whole DPDP regime. It does not distinguish between sensitive and non-sensitive health data. Nor does it address any of the specific concerns about the vulnerabilities of API-mediated transactions in the ABDM ecosystem, where consent, identifier, and clinical data flow through one and the same pipe.

Therefore, the 2025 Rules are necessary but not sufficient for the ABDM scenario. The former operationalises the general framework put into place by the latter. The former does not deal with the accountability issues specific to the health sector raised by the latter's architecture. As we know from experience, the pipe was always narrow. With the 2025 Rules in place, the pipe just carries more traffic in the same narrow walls.

C. The IT Act and the Transitional Regime

However, the IT Act introduces additional accountability systems for health data, but their continued relevance depends on a significant transitional period. According to Section 43A, companies that fail to observe 'reasonable security practices and procedures' during the handling of sensitive personal information can be penalized by the affected party through financial compensation. [33] The SPDI Rules made under this statute consider 'medical records and history' as sensitive Personal Information requiring extra security precautions. On the other hand, section 44(2) of the DPDP Act authorizes the deletion of Section 43A and SPDI Rules from May 13, 2027.[34] For all purposes up to this date, both the current IT Act regime and the new DPDP Act would apply simultaneously, possibly creating contradictory compliance standards.

There are two critical points about the transitional framework that require closer scrutiny. Firstly, Section 43A liability regime and SPDI Rules assumed a bilateral nature of the data transaction process and utilized security metrics such as ISO/IEC 27001, rather than multi-

[33] IT Act § 43A.
[34] DPDP Act § 44(2). Once § 43A is omitted in May 2027, the DPDP Act provides no equivalent private compensation remedy, only Board-imposed penalties under § 33.

party API transactions. Consequently, they fail to clarify how to assess reasonable security or assign liability whether to the at-fault entity, the current possessor, or all parties when multiple entities participate in a single data transaction. Second, the DPDP Act fundamentally fails to replicate Section 43A's private compensation remedy. Once Section 43A is omitted in May 2027, enforcement will rely exclusively on Board-imposed penalties, removing individuals' statutory right to compensation for data breaches. This represents a significant remedial regression for data principals harmed by API-mediated breaches. Although Section 72A remains active to provide criminal penalties for unauthorized data exposure, it offers no compensatory relief.[35]

D. Sector-Specific Instruments

The HDMP, issued in 2020 under the predecessor NDHM, establishes data governance principles within the ABDM ecosystem, including purpose limitation, data minimization, collection limitation, and security safeguards.[36] However, the HDMP is a policy document rather than a statutory instrument it lacks binding legal force independent of the IT Act and DPDP Act, and its enforcement mechanisms are limited to ecosystem-level sanctions such as revocation of ABDM registration. It does not create private rights of action for data principals.

Other instruments provide incremental regulation. The EHR Standards 2016 set out the technical requirements for EHR systems, but do not touch upon interoperability via APIs.[37] The Telemedicine Practice Guidelines 2020 regulate remote consultations; however, they remain silent about the underlying infrastructure of data exchange via API from teleconsultations to EHR databases. CERT-In Directions of April 2022 require reporting within six hours of cyber security incidents by any entity using computer systems, including those operating under the ABDM framework.[38] Finally, the Consumer Protection Act 2019 may cover the issue of product liability for the defective provision of digital health products: Section 84 et seq. impose liability for providing defective goods and deficient services, and a health application that results in injury to a patient as a result of defective software coding might be

[35] IT Act § 72A (not repealed by the DPDP Act; continues to provide criminal penalties of up to three years' imprisonment).
[36] HDMP, *supra* note 7, cls. 12, 18, 26.
[37] MINISTRY OF HEALTH & FAMILY WELFARE, ELECTRONIC HEALTH RECORDS STANDARDS FOR INDIA V2.0 (2016) [*hereinafter* EHR STANDARDS]; BD. OF GOVERNORS, MED. COUNCIL OF INDIA, TELEMEDICINE PRACTICE GUIDELINES (2020) [*hereinafter* TELEMEDICINE GUIDELINES].
[38] INDIAN COMPUT. EMERGENCY RESPONSE TEAM, Directions Under § 70B(6) of the IT Act (Apr. 28, 2022).

liable under this legislation.[39] However, the CPA 2019 was not tailored for the purpose of regulating the data ecosystem and fails to cover the specific issues of the API-based ecosystem: chain transactions, insufficient consent, and intermediaries.

Therefore, we face an incomplete regulatory ecosystem in which none of the instruments provides a comprehensive and unified regime of accountability with regard to API-mediated health data transactions. While the DPDP Act deals with data protection, the HDMP covers health data governance, CERT-In addresses reporting of cyber security incidents, and the CPA 2019 addresses issues of product liability, yet their cumulative operation leaves gaps in regulation.

IV. Identifying the Accountability Gaps

A. Liability Allocation in Chained API Transactions

The most significant accountability gap concerns the allocation of liability when harm occurs at an indeterminate point in a multi-party API chain. Consider a scenario in which a patient's diagnostic record is transmitted from a public hospital (HIP) through the Consent Manager to a private insurer (HIU), which forwards it via API to a claims processing sub-contractor, which in turn shares it with a wellness application. If the record is altered during transit, or accessed by an unauthorized third party at any node, the patient suffers harm but the existing framework does not specify how liability should be distributed.

The DPDP Act imposes obligations on each 'data fiduciary' independently but does not address joint or several liability, contributory fault, or chain-of-custody obligations specific to API-mediated data flows[40]. Moreover, the Act provides no private compensation right only Board-imposed penalties under section 33. During the transitional period until May 2027, section 43A continues to provide a compensation remedy, but it was designed for bilateral relationships and does not clarify whether liability attaches to the entity at fault, the entity in possession at the time of breach, or all entities in the chain. The HDMP contemplates 'accountability' as a principle but does not operationalize it into a liability mechanism.[41] The result is a doctrinal

[39] The Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019, §§ 2(7), 2(42), 84–87 (India) [*hereinafter* CPA 2019].
[40] Graham Greenleaf, *India's Digital Personal Data Protection Act 2023: The Long Road to Data Protection*, PRIVACY LAWS & BUS. INT'L REP., 2023, at 1, 6–8.
[41] HDMP, *supra* note 7, cl. 26.3.

vacuum: patients harmed by API-mediated breaches face the burden of identifying the responsible entity without statutory guidance on liability apportionment. The process becomes more difficult when it comes to API ecosystems, in which data undergoes encryption or decryption at several intermediate levels before reaching the end user. The technological challenge of identifying the flow of data through several chains of APIs adds another layer of complication to the already difficult task of establishing causality within the legal framework.[42]

B. Consent Inadequacy

Secondly, there is a discrepancy between the structure of the ABDM Consent Manager and the actual API-based mechanism of accessing the data. As mentioned earlier, the consent manager manages consent for categories of data and entities involved in their exchange: the patient consents to allow 'health records' to be shared with a certain HIU for a limited period of time. The actual mechanism of accessing those records, however, works on a much more granular level, allowing HIUs to extract particular FHIR resources such as diagnostic reports, medications, allergies, clinical notes, etc.[43]

The individual who consents to sharing his/her 'health records' with the insurance company may be unaware that such consent involves a process by which the API call extracts records regarding mental assessment, substance abuse treatment, HIV status and reproductive health, each type of record being distinct from the others in terms of its qualitative sensitivity. This leads to the crucial question of whether the consent obtained in respect of entity and category of information complies with the 'specific and informed' mandate of the DPDP Act. In view of the constitutionally required standard of proportionality, as enunciated by Puttaswamy, the answer to the above question cannot but be in the negative.[44] As argued by Saksena et al., this gap between technical and consented data granularity is an architectural problem of the API-based ecosystem for health data.

C. The Third-Party Regulatory Vacuum

Another regulatory gap exists for third-party applications like tech companies and wellness

[42] Rishi Saripalle et al., *Using HL7 FHIR to Achieve Interoperability in Patient Health Record*, 94 J. BIOMEDICAL INFORMATICS 103188 (2019).
[43] Saksena et al., *supra* note 9, at 4–6.
[44] Rahul Lakra & Ananya Shrivastava, *Confronting the Metadata Dilemma in India: A Turn to Context and Proportionality*, 32 INT'L J.L. & INFO. TECH. eaae012 (2024).

applications that use health data from ABDM APIs. Although strict regulation is exercised by the HDMP and applicable sector regulations for the main organizations, there is a drastic fall in regulation the moment the health data leaves for third party apps. The DPDP Act, in general, places all the third-party apps under data fiduciaries where they are subject only to the general security provisions, which have no context of the specific security considerations of the healthcare industry. Consequently, sensitive diagnostic data receives the same basic legal protection as an e-commerce delivery address.[45] Furthermore, the 2016 EHR Standards and 2020 Telemedicine Guidelines completely exclude these platforms.[46] Finally, while the ABDM Sandbox certifies initial technical integration, it mandates no continuous regulatory compliance.

This deficiency is particularly troubling considering the findings by independent cybersecurity studies, which have established that most third-party mobile healthcare applications, including those that might be able to connect to the ABDM APIs to obtain diagnostic or wellness data, lack security measures and fail even the minimum level of security tests. In a study conducted in 2021, which included an analysis of 30 mHealth apps, it was observed that 100% were susceptible to API attacks, with 77% leaking API keys and 7% having hardcoded usernames/passwords, potentially allowing unauthorized access to sensitive patient information such as records and pathology reports.[47] These issues, which expose data for millions of users, underscore how generic DPDP Act obligations may prove insufficient for healthcare-specific risks when third-party wellness platforms or tech firms access ABDM-linked data without sector-tailored, ongoing security mandates.

D. The Classificatory Gap: API Intermediaries

The DPDP Act splits organizations into just two camps data fiduciaries and data processors.[48] However, this black-and-white approach completely misses a unique group of entities that are

[45] Deepika Saluja et al., *Evolving Policy and Regulatory Landscape for Digital Health in India: A Narrative Review*, *in* COMPETITION AND REGULATION IN INDIA, 2023, at 85 (CUTS Int'l 2023).
[46] EHR STANDARDS, *supra* note 37; TELEMEDICINE GUIDELINES, *supra* note 37.
[47] Steve Alder, *100% of Tested mHealth Apps Vulnerable to API Attacks*, HIPAA J. (Feb. 16, 2021), https://www.hipaajournal.com/100-of-tested-mhealth-apps-vulnerable-to-api-attacks/; Dave Muoio, *Report: Patient Info at Risk Due to Rampant API Vulnerabilities Among Major Mobile Health Apps*, MOBIHEALTHNEWS (Feb. 9, 2021), https://www.mobihealthnews.com/news/report-patient-info-risk-due-rampant-api-vulnerabilities-among-major-mobile-health-apps.
[48] Jidesh Kumar, *The Future of Consent Management Under the DPDP Act & DPDP Rules: Redefining User Autonomy Through Consent Managers and Interoperable Platforms*, KING STUBB & KASIVA (Nov. 17, 2025); DPDP Act § 2(5) (defining 'Data Fiduciary'); *id.* § 2(12) (defining 'Data Processor'). The Act recognizes no intermediate category.

crucial to the ABDM ecosystem. We can essentially spot three types of *API intermediaries* that fall through the cracks. The first is the ABDM Consent Manager. Even though the DPDP Act legally categorizes it as a registered entity meant to enable consent management, on the ground, it really acts as a neutral gatekeeper rather than a purpose-setter. It controls the flow of data by checking consents and authorizing API transactions through digital artifacts, without having any say in *why* or *how* the data is ultimately used.[49] However, despite carrying out this restricted role, the law places upon Consent Managers the burden of similar to data fiduciaries considering that they are supposed to act in fiduciary capacity towards data principles. This leads to the conclusion that the regulatory requirements placed upon data fiduciaries are ill-fitting for a mere consent manager.

The second category of API intermediary is the ABDM Gateway Infrastructure. Every time a HIP communicates with an HIU using an API, it does so via this Gateway, which authenticates the data using security tokens to ensure encryption.[50] In other words, the ABDM Gateway functions merely as a secure router for transferring health data. It neither specifies the purposes for which the data must be processed nor serves as the data processor of any data fiduciary. Lastly, another type of actor to consider are downstream applications. In this case, the health data is processed by external platforms, which are unrelated to each other and to the parties granting consent for the data processing, resulting in complex issues of consent management and system interconnection. In one example, a patient grants their consent for sharing their medical record with Hospital X (HIU). Next, a wellness program created by a third party uses API access to access the patient's data. At no point is this third party functioning as a data processor for Hospital X. It uses the patient's consent as a basis for further operations but establishes its own purposes of the data processing. This classificatory gap is not merely taxonomic it is the root cause of the accountability deficit. The three gaps in Parts IV.A through IV.C each trace back to the mismatch between the DPDP Act's binary classification and the multi-layered reality of API-mediated ecosystems. Liability is indeterminate because the Act does not contemplate entities whose function is to facilitate rather than determine processing; consent is inadequate because the consent architecture does not differentiate between purpose-setting fiduciaries and consent-mediating intermediaries; and third-party applications fall into a regulatory vacuum because the Act offers no graduated obligations between full fiduciary

[49] Bamang Apo, *Digital Health and Artificial Intelligence: A Strategic Framework for India*, 14 INT'L J. RSCH. APPLIED SCI. & ENG'G TECH. (2026).
[50] Data Secure, *Health Data in the Spotlight: Aligning NDHM, DPDPA, and ABHA Frameworks*, DATA SECURE BLOG (July 14, 2025).

responsibility and mere processor status. Neither the GDPR's framework for controllers and processors nor EU academic research has completely addressed the similar issue. However, the Article 29 Working Party has recognized that entities involved in defining the means and purposes of data processing do so to varying extents.[51]

V. Comparative Perspectives

A. The EHDS[52]

At present, the EHDS Regulation provides the most extensive rule-book on achieving interoperability for health data. It has three distinct characteristics. Firstly, it draws a sharp distinction between the purpose for which the data can be used distinguishing between 'primary use,' i.e., the data usage for patient care and 'secondary use,' for example, in the case of innovation. As a consequence, different access rules can be applied to both kinds of uses, thus creating legal certainty for the EHDS.[53] This is another point where Indian ABDM seems deficient as it fails to differentiate between clinical, administrative, research, and business-related uses of health data acquired by way of API.[54] Secondly, EHDS Regulation places responsibility for ensuring high-quality data with data providers.[55] They must make sure that all shared data is correct, complete, and updated. The third characteristic of the EHDS framework is its provision for the certification and labelling of EHR systems. This approach gives an opportunity for upfront control of EHR's quality, and such a system can also be implemented in Indian ABDM sandbox. Additionally, EHDS provides for the establishment of specific organizations responsible for handling health data access. Ultimately, the EHDS proves that effectively governing health data sharing requires specialized institutions, rather than just relying on broad, general-purpose data protection authorities. [56]

While the EHDS doesn't directly solve the issue of classifying API intermediaries discussed earlier, its tailored rules for data holders, access bodies, and EHR manufacturers show us

[51] Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 82(4)–(5), 2016 O.J. (L 119) 1 [*hereinafter* GDPR]. *See also* Art. 29 Data Prot. Working Party, *Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'* (WP 169, 2010), at 24–27.
[52] Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space, 2025 O.J. (L) [*hereinafter* EHDS Regulation].
[53] EHDS Regulation, *supra* note 52, arts. 33–36.
[54] Shravishtha Ajaykumar et al., *The Digital Personal Data Protection Act, 2023: Recommendations for Inclusion in the Digital India Act*, OBSERVER RSCH. FOUND. (Oct. 2023).
[55] EHDS Regulation, *supra* note 52, art. 55.
[56] *Id.* arts. 53–65.

exactly how to move beyond simple, black-and-white legal classifications and build a system of multi-layered accountability.

B. The United States ONC Framework

The 21st Century Cures Act required patient access to their health records via APIs using the FHIR standard.[57] The ONC rule set out conditions relating to certification criteria, information blocking, and exceptions.[58][59] There are two aspects which are quite relevant. First, the information blocking clause imposes positive duties against unreasonably hindering the exchange of data using APIs, which is an aspect not covered by the Indian scheme, i.e., ensuring proper handling of data as opposed to improper handling of data. Secondly, there are eight exceptions to the prohibition on information blocking.

Secondly, the experience of the US has resulted in a lot of empirical data on failure cases of the implementation of FHIR APIs: 60 percent of tested APIs were found to be open to exploitation, over 50 percent of healthcare applications were seen to include hardcoded credentials, and none of the mobile applications tested prevented person-in-the-middle attacks.[60] The ONC's subsequent engagement with the OWASP API Security framework[61] demonstrates that API security governance requires continuous, technically informed regulatory attention rather than static certification a lesson directly applicable to ABDM's sandbox approval process.

VI. Toward Layered API Accountability

A. Recognizing the API Intermediary

The starting point for the framework is the acknowledgment that the distinction in the DPDP Act between "fiduciary" and "processor" needs to be augmented with a third type – that of the "API intermediary." An API intermediary is any party that manages either the conditions, routing, authentication, or consent mediation relating to the movement of Personal Information

[57] 21st Century Cures Act, Pub. L. No. 114-255, § 4004, 130 Stat. 1033 (2016).
[58] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642, 25,665–72 (May 1, 2020).
[59] 45 C.F.R. pt. 171 (2020) (information blocking exceptions).
[60] ALISSA KNIGHT, PLAYING WITH FHIR: HACKING AND SECURING FHIR API IMPLEMENTATIONS 8–18 (Approov 2021).
[61] *Unlocking the Future of API Security in Healthcare*, ONC HEALTH IT BUZZ (Aug. 7, 2023), https://www.healthit.gov/buzz-blog/privacy-and-security/unlocking-the-future-of-api-security-in-healthcare.

between fiduciaries via APIs but does not decide on the underlying purpose of the data processing. This includes Consent Managers (which decide if data flows by verifying the consent artifacts and issuing authorization tokens), ABDM Gateway (which manages routing, session handling, and authentication), and derivative consent managers (using the data accessed under consent granted by another entity).

There are three major implications of this definition from a legal standpoint. Firstly, intermediaries need custom tailored liability standards – they are to be responsible for those things that they control and have control over, namely, the security of consent artifact, transit and authentication security, but not the substantive integrity of health records nor the quality of the original consent. Secondly, consent obligations must vary – the duty of intermediaries consists in proper implementation of consent parameters rather than obtaining consent or deciding on the scope of consent. Finally, there is a need to distinguish security obligations, and make them related to transit security and authentication rather than purpose limitation, which belongs to the substantive data fiduciary. The problem with not defining intermediary is that the law will impose inappropriate fiduciary and processor roles onto those institutions, leading to mismatch between obligations and responsibilities mentioned above in Part IV.

B. Proportional Liability

Liability should be distributed in proportion to each participant's degree of control over the data at the relevant stage of the API transaction, drawing on the *Puttaswamy* proportionality standard[62] and the Consumer Protection Act 2019's product liability framework.[63] HIPs bear primary liability for data accuracy and completeness at the point of origin; the Consent Manager bears liability for the integrity of consent artefacts and accurate reflection of the data principal's authorization;[64] HIUs bear liability for purpose compliance, security of received data, and ensuring that downstream processing does not exceed the consented scope; and any entity that processes health data beyond the original consent scope bears full fiduciary liability regardless of its intermediary status[65]. This approach ensures that the intermediary classification cannot become a shield for entities that exceed their authorized function an entity

[62] *Puttaswamy*, (2017) 10 SCC 1, ¶ 180 (Chandrachud, J.).
[63] CPA 2019 §§ 84, 86.
[64] HDMP, *supra* note 7, cl. 12.2.
[65] Lipsa Aggarwal & Mrinmoy Roy, *A Strategic Roadmap to the Successful Implementation of Digital Health Records in India*, *in* UNITING KNOWLEDGE INTEGRATED SCIENTIFIC RESEARCH FOR GLOBAL DEVELOPMENT 11 (Seven Editora 2023).

that begins as an intermediary but determines its own processing purposes transitions to full fiduciary accountability by operation of law.

GDPR's joint and several liability framework in articles 82(4) and 82(5) makes for an excellent comparison tool in cases of ambiguous causation. In this context, where it is impossible to ascertain at what point in the process of the API chain a harmful occurrence takes place, all stakeholders involved in the process must be jointly and severally liable, with a right of contribution amongst themselves. Importantly, the framework must incorporate a private right to compensation that can be enforced against the Data Protection Board since the omission of section 43A of the IT Act in May 2027 would result in a lack of redressability on the part of data principals.

C. Purpose-Bound Granular Consent

The consent principle addresses the structural mismatch identified in Part IV.B by requiring that consent be aligned with specific FHIR resource categories rather than broad data types. The ABDM HIE-CM currently operates at the HI-Type (document-bundle) level, meaning consent is granted for categories such as 'DiagnosticReport' or 'Prescription' rather than for individual FHIR resources within those bundles.[66] The proposed framework requires that sensitive health data categories mental health records, substance abuse treatment data, HIV/STI status, and reproductive health information be subject to separate, unbundled consent that cannot be combined with general health record access.

This principle enjoys substantial support from two Indian laws, which make the need for significantly higher levels of unburdened consent for processing sensitive information related to health extremely clear. The first of these can be exemplified by the Mental Healthcare Act 2017. As per Section 23 of this Act, there is no necessity for the individual affected by a mental disorder to disclose his or her status related to mental well-being to anyone except for his/her own healthcare professionals.[67] The same type of measure is present in the HIV/AIDS Act of 2017, which requires all such health data to be shared only after obtaining prior consent, and this obligation comes along with strict repercussions that include legal punishment for leaking this health data without consent. These acts recognize that health data belongs to certain

[66] ABDM HIE-CM SPECIFICATION, *supra* note 16.
[67] CUTS INT'L, COMPETITION AND REGULATION IN INDIA, 2023: REGULATORY DEFICIT IN ACCESS TO EQUITABLE HEALTHCARE 111–12 (2023).

categories, which need to be considered separately while dealing with consent.[68] EHDS's differentiation between primary/secondary use cases once again illustrates how effective differentiated consent models can be applied at large scale. The EHDS technical framework mandates that an API access token scope cannot extend beyond the data elements that the data subject has explicitly provided consent for, thereby avoiding the prevalent practice where broad consent is granted to fetch data that goes well beyond consented-for categories.[6970] This ensures that the DPDP Act's requirement for "specific" and "informed" consent will be fulfilled at the level of the API implementation. It is critical to match consent granularity with the design of the API because otherwise, while compliance with the consent requirements of the DPDP Act can still be achieved in a formal sense, its actual purpose would be defeated.

D. Mandatory Security-by-Design

The security-by-design principle addresses the documented vulnerability landscape of health data APIs. Every participant in the ecosystem must adopt security measures that correspond to the sensitivity of the data they handle. Additionally, DPDP Rules 2025 prescribe general security measures under rule 6, but dropped the former SPDI Rules' explicit mandate to comply with ISO/IEC 27001 arguably a regulatory regression.[71] The former SPDI Rules, rule 8(2), had required compliance with ISO 27001 as the benchmark for 'reasonable security practices and procedures.' The DPDP Rules replaced this with self-defined measures, omitting all reference to international standards.[72]

The proposed framework seeks to correct this regression by anchoring security-by-design obligations to internationally recognized health-sector standards, principally ISO 27799:2025, which provides healthcare-specific implementation guidance for information security controls applicable to electronic health record systems, medical devices, and API-mediated data exchange.[73] Comparatively, the United States' NIST SP 800-66r2 (2024) maps healthcare

[68] ORG. FOR ECON. CO-OPERATION & DEV., HEALTH DATA GOVERNANCE: PRIVACY, MONITORING AND RESEARCH (2015).
[69] EUROPEAN COMM'N, IMPACT ASSESSMENT REPORT ACCOMPANYING THE PROPOSAL FOR A REGULATION ON THE EUROPEAN HEALTH DATA SPACE (2022).
[70] Sophie Dramé-Maigné et al., *Reviewing Access Control Solutions for the IoT Through the Prism of Architecture*, 54 ACM COMPUTING SURVEYS, art. 138, at 7–8 (2021), https://doi.org/10.1145/3465170.
[71] DPDP Rules, *supra* note 32, r. 6. The former SPDI Rules mandated ISO/IEC 27001 compliance; the DPDP Rules dropped all international standards references.
[72] INT'L ORG. FOR STANDARDIZATION, ISO/IEC 27001:2022 INFORMATION SECURITY MANAGEMENT SYSTEMS REQUIREMENTS (2022).
[73] INT'L ORG. FOR STANDARDIZATION, ISO 27799:2025 HEALTH INFORMATICS INFORMATION SECURITY CONTROLS IN HEALTH BASED ON ISO/IEC 27002 (2025).

security requirements to the NIST Cybersecurity Framework 2.0, providing a granular operational model for health data API security that India's framework could adapt.[74] Specific requirements should involve end-to-end encryption, certificate validation, limited access tokens with required maximum validity periods, ongoing vulnerability scanning with mandatory notification to CERT-In and the NHA, and regular security assessments with suspension of API usage in case of violations. On the part of API intermediaries, other responsibilities should involve tamper-resistant logging of all consents managed and authentications performed. Any technical standards need to be formulated based on the OWASP API Security Top 10, wherein one such example in case of API security flaw within healthcare is the broken object-level authorization (BOLA). Attacks exploiting broken object-level authorization (BOLA) can take place since hackers can access data belonging to other users through the object IDs being used during the API requests.[75] For instance, in a healthcare context, if a user has access rights to view their own health records through the API endpoints provided, then this very endpoint can be exploited by an attacker to retrieve the health data belonging to anyone else. The six-hour reporting rule of CERT-In shall serve as a base for formulating the incident response strategy, which in turn must be supplemented by sector-wise reporting to the NHA.[76]

E. Illustrative Draft Provision

The following provision, proposed for rules under DPDP Act section 36, demonstrates how the framework can be operationalized:

> ***'Section [X]. Accountability for API-mediated health data processing.***
>
> *(1) In this part, the phrase "API intermediary" will refer to any individual, organization, or other party that regulates the terms, routing, authentication, or mediation of consent concerning the movement of Personal Information through Application Programming Interfaces (APIs) between Data Fiduciaries without defining the intended purpose of the processing. An API intermediary cannot be categorized as*

[74] NAT'L INST. OF STANDARDS & TECH., SP 800-66R2, IMPLEMENTING THE HIPAA SECURITY RULE: A CYBERSECURITY RESOURCE GUIDE (Feb. 2024).
[75] OWASP FOUND., *OWASP API Security Top 10 2023*, https://owasp.org/API-Security/editions/2023/en/0x11-t10/.
[76] DPDP Act § 36 (rule-making power); § 36(2)(m) (rules relating to 'reasonable security safeguards' under § 8(4)).

a Data Fiduciary or Data Processor based on its role as an intermediary in the data transaction.

(2) For a chained API transfer, liability in the event of damage will be shared by all parties in line with their respective levels of control: the originating Data Fiduciary will be liable for data accuracy; the recipient Data Fiduciary will be liable for purposeful and secure data processing; the API intermediary will be liable for data artifact validity and security during the transmission process but not for the actual accuracy of data and the validity of the consent given; and any party that performs additional data processing beyond the consent will be fully responsible for the fiduciary responsibility. Where causality is ambiguous, all parties involved will be jointly and severally liable, with the right of contribution reserved.

(3) The consent form for accessing health information through APIs must outline what the various classes of health information are and what is intended to be done with each class, along with disclosing whether the information will be shared elsewhere. The access to health data in any sensitive class requires unbundled consent.

(4) Participants shall take necessary security measures in accordance with ISO 27799:2025 or comparable standards such as encryption, certificate validation, scoped token, continuous monitoring, and audit. The API intermediaries should ensure tamper-proof logging of all consents and authentications activities.'

This clause will be implemented as rules under Section 36 of the DPDP Act so that there would not be any need to amend the core legislation. There are four clauses corresponding to the four elements of the layered framework: classificatory recognition (clause 1), proportional liability with a private right to compensation (clause 2), purpose-specific consent that can be unbundled into sensitive categories (clause 3), and security-by-design obligations consistent with international standards (clause 4). The application scope of this rulemaking clause is limited only to health data processing through APIs in the ABDM ecosystem, thus making it possible to avoid a far more contentious and expansive reform of the DPDP Act's provisions. The sectoral approach adopted by this proposal finds a basis in Section 36(2)(m) of the DPDP Act, according to which the Central Government is empowered to define "reasonable security safeguards" in rules.

VII. Conclusion

This research reveals that the classification flaw in the existing legal regime, which is scattered over the DPDP Act, the IT Act, the HDMP, and sectoral laws, is evident from the following. The binary classification under the DPDP Act, of 'data fiduciaries' and 'data processors,' does not reflect the existence of separate functional categories of 'APIs' (Consent Managers, gateways, derivative consent), that form a part of the ABDM architecture.[77]

This classificatory gap is the root cause of three derivative accountability deficits: indeterminate liability in chained API transactions, structurally inadequate consent mechanisms, and a regulatory vacuum governing third-party applications.[78] The proposed 'layered API accountability' framework addresses the root cause by recognizing the API intermediary as a new legal category with bespoke obligations, and derives three operational principles: proportional liability allocating responsibility according to degree of control; purpose-bound granular consent aligned with FHIR resource categories and requiring unbundled authorization for sensitive health data categories; and mandatory security-by-design anchored to international standards, principally ISO 27799:2025.

Such principles could be implemented using delegated legislation under DPDP Act Section 36 without any change to primary legislation as shown in the sample draft provision under Part VI.E. The impending deletion of Section 43A from IT Act in May 2027, resulting in the loss of the only existing private compensation regime for data breaches, adds significance to this matter. The framework outlined herein provides for an actionable roadmap to addressing the accountability gap issue before it gets out of hand, providing for a legal architecture to match the scope and magnitude of India's health IT structure. In future studies, there should be a convergence toward examining the capability of institutions like NHA and the Data Protection Board in implementing the framework, analysing the real-world security performance of ABDM APIs, as well as learning from similar challenges encountered in other digital health systems across the world, such as NHS Digital in the UK and the My Health Record program in Australia. While the classification of API intermediaries has been done in the context of health data, it is worth noting that this challenge is not confined to health data alone but can affect any system that uses APIs where the data protection binary is inadequate.

[77] *Puttaswamy*, (2017) 10 SCC 1, ¶¶ 325–28 (Chandrachud, J.).
[78] PRIVACY IN PRACTICE: STRATEGIES FOR DATA MANAGEMENT IN INDIA 67–81 (Kazim Rizvi & Shravishtha Ajaykumar eds., Observer Rsch. Found. 2025), https://www.orfonline.org/research/privacy-in-practice-strategies-for-data-management-in-india.