Page 2071 - 2091

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

AI-Driven Healthcare Diagnostics and Data Privacy: Legal Challenges of Secondary Use of Patient Data

GARGI SINGH* AND DR. UTKARSH VERMA**

ABSTRACT

Artificial intelligence is fundamentally reordering the landscape of healthcare diagnostics. AI-driven systems now perform radiological image analysis, pathological screening, genomic interpretation, predictive risk stratification, and clinical decision support at a scale and speed that surpasses conventional clinical capacity. Yet every AI diagnostic system is, at its foundation, a data system: its performance depends upon access to vast repositories of historical patient data, namely records, images, biomarkers, and treatment outcomes, collected for clinical care but deployed for computational learning. This paper examines the legal challenges arising from the secondary use of patient data for AI diagnostic development and deployment, with particular focus on India's evolving regulatory architecture. Anchored in the constitutional right to privacy as confirmed in Justice K.S. Puttaswamy (Retd.) v. Union of India, the analysis traverses the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, the sector-specific health data governance framework, and the comparative regimes of the European Union (including the EU AI Act, 2024, the GDPR, and the European Health Data Space Regulation, 2025) and the United States under HIPAA. Drawing upon the latest case law, including the landmark Lokken v. UnitedHealth Group litigation advancing in the District of Minnesota, the record 2025 HIPAA enforcement actions of the Office for Civil Rights, and emerging constitutional challenges before the Supreme Court of India, the paper argues that India's current legal framework is structurally inadequate to govern the secondary use of patient data for AI, and proposes a comprehensive rights-based regulatory architecture.

I. INTRODUCTION

The relationship between artificial intelligence and healthcare diagnostics is no longer aspirational: it is operational. Across India's hospital networks, diagnostic imaging centres, genomics laboratories, and telehealth platforms, AI-based tools are now performing tasks that

* Author is a Ph.D. Research Scholar at National University of Study and Research in Law (NUSRL), Ranchi, Jharkhand, India.

** Author is an Assistant Professor of Law at National University of Study and Research in Law (NUSRL), Ranchi, Jharkhand, India.

 [ISSN 2581-5369]

define clinical medicine: detecting malignant lesions in CT scans, flagging sepsis risk from electronic health records, stratifying patients by cardiac event probability, and suggesting treatment pathways from pharmacogenomic profiles. The National Health Authority's Ayushman Bharat Digital Mission has created over 730 million Ayushman Bharat Health Account records,[1] linking patients' clinical histories across providers through a nationally unique health identifier, and creating precisely the kind of longitudinal, population-scale dataset upon which high-performing AI diagnostics depend. AI has an adoption rate of approximately 68 per cent in Indian healthcare, yet over 92 per cent of these deployments function in the absence of a dedicated legal regulatory framework.[2]

The legal challenge at the heart of this paper is specific and urgent: when patient data is collected in a clinical encounter for diagnosis, treatment, and care, and is subsequently used to train, validate, or commercially deploy an AI diagnostic system, what legal obligations govern that secondary use? Who must consent, and to what? What rights does the patient retain over data collected from their body and used to generate commercial value for the system developer? Who bears liability when the AI system trained on that data produces an erroneous diagnosis or an arbitrary clinical determination? And does India's current legislative and regulatory architecture provide constitutionally adequate answers to these questions?

These questions are not theoretical. The United States is currently witnessing the most consequential judicial examination of them: *Estate of Gene B. Lokken v. UnitedHealth Group, Inc.*,[3] a class action in the District of Minnesota alleging that UnitedHealth's AI model nH Predict, trained on six million patients' data, produced arbitrary, systemically inaccurate coverage determinations for Medicare Advantage members, with a 90 per cent appeal-reversal rate, overriding treating physicians' recommendations. As of April 2026, the court has ordered UnitedHealth to produce tens of thousands of AI-related documents, and the case is defining the boundaries of AI liability in healthcare. In California, a separate class action alleges that an AI clinical documentation tool recorded patient-clinician conversations without consent and transmitted them to third-party servers.[4] In India, constitutional challenges are gathering: the

[1] NATIONAL HEALTH AUTHORITY, AYUSHMAN BHARAT DIGITAL MISSION: ANNUAL REPORT 2024–25 (2025) [hereinafter *ABDM Report*] (reporting 730 million Ayushman Bharat Health Account (ABHA) records created and linked to a national unique health identifier).

[2] Shailendra Kumar & Priya Nair, *AI-Driven Healthcare in India: Legal Challenges and the DPDP Framework*, 4 INT'L J. TRENDS EMERGING RSCH. & DEV. 112, 115–17 (2025) (documenting a 68% AI adoption rate in Indian healthcare diagnostics, with over 92% of deployments functioning without a dedicated legal framework).

[3] *Estate of Gene B. Lokken v. UnitedHealth Grp., Inc.*, No. 0:23-cv-03514 (D. Minn. Feb. 13, 2025) [hereinafter *Lokken*] (granting in part and denying in part the motion to dismiss; allowing breach of contract and breach of the implied covenant of good faith and fair dealing to proceed).

[4] *Sutter Health & Me v. Doe*, No. 3:26-cv-01842 (N.D. Cal. filed Apr. 2026) (class action alleging that an AI clinical documentation tool recorded patient-clinician conversations and transmitted audio to third-party servers without

Supreme Court in February 2026 received a challenge to the DPDP Act's surveillance-enabling exemptions,[5] and the Central Drugs Standard Control Organisation's draft guidance on AI/ML-based medical devices, released for comment in 2025, proposes pre-market review requirements that have not yet been formally enacted.[6]

India's position is simultaneously one of extraordinary opportunity and acute legal vulnerability. The country's demographic scale, disease-burden diversity, and digital health infrastructure create conditions for AI diagnostic development that could transform healthcare access for hundreds of millions of people. But that same infrastructure is assembling patient datasets of unprecedented scope under a legal framework whose capacity to protect patients' constitutional rights has not been tested, and whose design, as this paper demonstrates, contains structural inadequacies that will become legally acute as AI diagnostics move from pilot to population-scale deployment.

II. Conceptual foundations: secondary use, data governance, and legal theory

A. Defining Secondary Use

In healthcare data governance, 'primary use' refers to the processing of patient data for the direct clinical purpose for which it was collected: diagnosis, treatment, care, and clinical communication. 'Secondary use' refers to any processing of that data for a purpose beyond the immediate clinical encounter: research, quality improvement, public health surveillance, commercial product development, insurance underwriting, and, most significantly for this paper, the training, validation, and deployment of AI diagnostic systems. The distinction is not merely taxonomic; it is constitutionally and legally foundational. The consent given by a patient at the point of clinical care, often obtained through a standard admission form, is directed at the primary use of their data for treatment. It does not, absent specific disclosure and affirmation, extend to secondary processing for commercial AI development.

consent; asserting violations of the federal Wiretap Act, 18 U.S.C. § 2511, and the California Confidentiality of Medical Information Act, Cal. Health & Safety Code § 56 et seq.).

[5] Digital Personal Data Protection Act, No. 22 of 2023, § 17(2)(a)–(b), Acts of Parliament, 2023 (India) [hereinafter *DPDP Act*]; id. § 17(3); see *Reporters' Collective v. Union of India*, W.P. (C) No. 130/2026 (India) (constitutional challenge pending as of June 2026, contesting the breadth of the exemptions and the RTI-curtailment provisions).

[6] Central Drugs Standard Control Organisation, Digital Health Technologies: Guidance on Artificial Intelligence/Machine Learning (AI/ML)-Based Medical Devices (Draft Guidance, 2025) [hereinafter *CDSCO AI Draft Guidance*] (proposing pre-market review, clinical validation, algorithmic transparency reporting, bias assessment, and post-market surveillance; yet to be formally notified).

 [ISSN 2581-5369]

The DPDP Act, 2023 codifies this distinction in Indian law: Section 8(1) prohibits data fiduciaries from using personal data beyond the stated purpose of collection,[7] and the KPMG Healthcare Report confirms that secondary use without consent is prohibited.[8] Yet the gap between this statutory prohibition and the reality of healthcare data flows in India is substantial. Hospital systems routinely aggregate patient records for 'quality improvement' or 'operational analytics'; health-tech startups license clinical datasets for AI model training; and the Ayushman Bharat Digital Mission's linked records create population-scale health data repositories whose secondary-use governance remains governed by administrative policy rather than enforceable statute.[9]

B. Data Governance Theories

The theoretical frameworks for health data governance fall into three broad paradigms, each with distinct legal implications. The *property-based* paradigm treats health data as a form of personal property over which the individual patient has exclusive rights, including the right to alienate through licence or to exclude through withholding consent. This paradigm, reflected in the DPDP Act's consent architecture, provides the strongest protection against secondary use but may impede population-scale research that generates public health benefits from data aggregated beyond any individual's clinical context.

The *relational privacy* theory, developed by scholars including Nissenbaum through the lens of contextual integrity, argues that privacy is violated not merely by disclosure but by the violation of contextual norms governing information flow. Under this theory, health data flows appropriately when they match the norms of the context in which the data was shared, the clinical encounter, but are violated when data is transferred to an entirely different social context, such as commercial AI development, without adequate alignment with the patient's reasonable expectations.[10]

The *surveillance capitalism critique* advanced by Zuboff identifies a structural problem that transcends individual consent: the commodification of personal health data by technology

[7] *DPDP Act*, *supra* note 5, § 8(1) (purpose limitation: data may be used only for the purpose for which consent was given).

[8] KPMG INDIA, THE PRIVACY PRESCRIPTION: IMPACT OF THE DPDP ACT AND RULES IN THE HEALTHCARE AND LIFE SCIENCES SECTOR (Dec. 2025) [hereinafter *KPMG Healthcare Report*] (noting that the consent framework prohibits secondary use without fresh, specific, and revocable consent, and that blanket or implied consent in hospital intake forms is expressly invalid).

[9] AYUSHMAN BHARAT DIGITAL MISSION HEALTH DATA MANAGEMENT POLICY, 2023 [hereinafter *ABDM Policy*] (prohibiting secondary use of health records without fresh, granular consent; requiring Health Information Providers and Users to register with the National Health Authority).

[10] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 56–60 (2015); see also VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 147–51 (2018).

 [ISSN 2581-5369]

companies for AI model training constitutes a unilateral expropriation of patients' medical experience that produces power asymmetries inconsistent with democratic health governance.[11] This critique has direct purchase in the Indian context, where large health-tech platforms and digital health aggregators are building patient datasets that will be used to train diagnostic AI systems, generating commercial value from data whose subjects received no share of that value and, in many cases, are unaware of the processing.

C. The De-identification Fallacy and the Re-identification Problem

A widely invoked legal justification for the secondary use of health data for AI training is that the data has been 'anonymised' or 'de-identified,' removing the legal protections that apply to personal data. This justification has been comprehensively challenged in the technical literature. Ohm's foundational work demonstrated that re-identification of ostensibly anonymised health datasets is feasible through cross-referencing with auxiliary data, and Sweeney demonstrated that 87 per cent of the US population can be uniquely identified from ZIP code, birth date, and sex, three fields routinely present in 'anonymised' medical records.[12] The implications for AI training datasets are acute: AI systems trained on 'de-identified' health data may generate outputs, including diagnostic predictions, risk scores, and pharmacogenomic recommendations, whose back-calculation reveals individual patients' identities, medical conditions, and treatment histories. The legal framework must therefore regulate 'anonymised' health data used for AI training on the basis of its actual re-identification risk, not its nominal anonymisation status.

III. India's Legal and Regulatory Framework Governing Health Data and AI Diagnostics

A. The Constitutional Foundation

The constitutional foundation for health data privacy in India is Articles 14, 19, and 21, as interpreted through the *Puttaswamy* judgments. *Puttaswamy I* (2017) established privacy as a fundamental right under Article 21 and articulated the four-part proportionality test (legality, legitimate aim, necessity, and proportionality) that any state or state-enabled intrusion into personal data must satisfy.[13] *Puttaswamy II* (2018), the Aadhaar judgment, reinforced that

[11] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 93–95 (2019).

[12] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716–18 (2010); Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, 3 Health (N.Y.) 1, 2–3 (2000) (87% of the U.S. population uniquely identifiable from ZIP code, birth date, and sex).

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 [hereinafter *Puttaswamy I*] (privacy as a fundamental right under Article 21; four-part proportionality test of legality, legitimate aim, necessity, and proportionality).

 [ISSN 2581-5369]

biometric and health data collection by the state must satisfy purpose limitation and data minimisation as constitutional requirements.[14] Article 14's guarantee of non-arbitrariness extends to algorithmic healthcare decisions: where an AI system makes a diagnostic or coverage determination affecting a patient's health or life without explainable, contestable reasoning, the determination is constitutionally arbitrary.[15]

B. The Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025

The DPDP Act, 2023, India's first comprehensive data protection statute, operationalises *Puttaswamy*'s constitutional mandate. Its core provisions directly govern AI-driven health data processing.

Consent architecture (Sections 5 to 8). Consent must be 'free, specific, informed, unconditional, and unambiguous, through a clear affirmative action.' The DPDP Rules, 2025, notified on November 14, 2025, require consent notices to be standalone, written in plain language, available in all 22 Scheduled languages of India, and to specify the exact data collected, purpose, and patient rights. Blanket or implied consent, as routinely obtained through hospital admission forms, is expressly invalid. This has immediate implications for health-tech companies whose current consent frameworks purport to cover both primary clinical use and secondary AI training through a single, undifferentiated clause.[16]

Purpose limitation, data minimisation, and storage limitation (Section 8). The Act prohibits use of personal data beyond the stated purpose of collection, requires that only data necessary for the stated purpose be collected, and mandates erasure upon withdrawal of consent or fulfilment of purpose.[17] For AI diagnostic developers holding patient datasets, the storage-limitation obligation creates compliance challenges: AI model training requires large historical datasets whose retention beyond the original clinical purpose may violate Section 8(7) absent a specific legal basis for extended retention.[18]

---

[14] *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2018) 16 S.C.C. 409 [hereinafter *Puttaswamy II*] (upholding the Aadhaar architecture subject to conditions; reiterating purpose limitation, proportionality, and data minimisation as constitutional requirements).

[15] INDIA CONST. art. 14; *State of West Bengal v. Anwar Ali Sarkar*, A.I.R. 1952 S.C. 75 (India) (Article 14 prohibits discriminatory and arbitrary state and quasi-state action).

[16] *DPDP Act*, *supra* note 5, § 6(1) (consent must be free, specific, informed, unconditional, and unambiguous); id. § 6(4); Ministry of Electronics & Information Technology, The Digital Personal Data Protection Rules, 2025, G.S.R. 747(E) (Nov. 14, 2025) [hereinafter *DPDP Rules 2025*], Rule 3 (notices to be standalone, in plain language, and available in all 22 Scheduled languages).

[17] *DPDP Act*, *supra* note 5, § 6(1); *DPDP Rules 2025*, *supra* note 16, Rule 3.

[18] *DPDP Act*, *supra* note 5, §§ 8(1), (3), (7) (purpose limitation, data minimisation, storage limitation); *KPMG Healthcare Report*, *supra* note 8.

 [ISSN 2581-5369]

Data Principal rights (Sections 11 to 13). Patients have rights to access their data, to correct inaccuracies, and to erase data and withdraw consent. The right to erasure has particular resonance in AI health data contexts: if a patient withdraws consent and demands erasure, the data fiduciary must not only delete the raw data but must also address whether the AI model trained on that data, and its ongoing deployment, continues to embody the patient's information in its parameters.

Significant Data Fiduciary obligations (Section 10 and DPDP Rules, Rule 12). Large hospital chains and major health-tech platforms are likely to be designated as Significant Data Fiduciaries under Section 10, triggering obligations including annual Data Protection Impact Assessments, independent audits, and algorithmic fairness assessments.[19] These obligations, once notified, would provide the primary regulatory mechanism for oversight of AI diagnostic systems processing patient data at scale.

Penalties (Section 33). The DPDP Act imposes financial penalties of up to INR 250 crore per violation; up to INR 200 crore for failure to take reasonable security safeguards causing a data breach; and up to INR 200 crore for failure to notify the Data Protection Board of a breach.[20]

C. State Exemptions and Structural Gaps

Section 17 of the DPDP Act creates sweeping exemptions for state processing of personal data, covering sovereignty, national security, and law enforcement purposes.[21] These exemptions are constitutionally suspect under the *Puttaswamy* proportionality framework and practically significant for health data governance: government hospitals, the National Health Authority's ABDM infrastructure, and public health research institutions fall outside many of the Act's accountability obligations by virtue of the Section 17 exemptions. A regime that protects patients from secondary use by private health-tech companies while leaving government health data systems largely unaccountable is neither constitutionally coherent nor functionally adequate.

A critical gap in the DPDP Act is the absence of any special category regime for health data. Earlier versions of India's data protection legislation, the Personal Data Protection Bill, 2019, explicitly designated health and genetic data as 'sensitive personal data' requiring heightened

[19] *DPDP Rules 2025*, *supra* note 16, Rule 12 (annual Data Protection Impact Assessments and independent audits for Significant Data Fiduciaries); Rule 7 (algorithmic fairness assessments); Rule 22 (breach notification within 72 hours).
[20] *DPDP Act*, *supra* note 5, § 16 (Data Protection Board of India); § 33 (penalties: up to INR 250 crore per violation; up to INR 200 crore for failure of reasonable security safeguards causing a breach; up to INR 200 crore for failure to notify the Board); § 40 (appellate jurisdiction).
[21] *DPDP Act*, *supra* note 5, § 17(2)–(3); *Reporters' Collective v. Union of India*, W.P. (C) No. 130/2026 (India) (pending).

 [ISSN 2581-5369]

protection. The enacted DPDP Act, 2023, retreated from this position, treating health data as ordinary personal data subject only to the general consent and purpose limitation framework. This structural decision creates a significant lacuna: the particular vulnerabilities associated with health data, including its potential for re-identification, its implications for insurability and employment, its intimate connection to bodily autonomy, and its capacity to reveal family genetic information, are not addressed by any heightened protection under the DPDP Act.

D. Sector-Specific Legal Framework

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) remain operative alongside the DPDP Act pending formal amendment. The SPDI Rules explicitly designate health and medical records as 'sensitive personal data' and require mandatory written informed consent from the provider before collection, restriction of disclosure to third parties without prior permission, and use of the data only for the purpose for which it was collected.[22]

The Clinical Establishments (Registration and Regulation) Act, 2010 (CERA) and the Medical Council of India's Professional Conduct Regulations, 2002 impose record-keeping and patient-confidentiality obligations on registered clinical establishments and medical practitioners.[23] The Medical Devices Rules, 2017 define 'software intended for diagnosis or treatment' as a medical device, thereby capturing AI-based diagnostic software, and impose Class A to D risk classification requirements with corresponding conformity-assessment obligations.[24] Class C and D AI diagnostic software require clinical investigation prior to market authorisation, a standard that the majority of currently deployed AI diagnostic tools in India have not met.

The Ayushman Bharat Digital Mission Health Data Management Policy, 2023 and the National Digital Health Blueprint govern consent-based sharing of digital health records through the

[22] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3 [hereinafter *SPDI Rules*] (health and medical records listed as sensitive personal data); Rule 5(1) (written informed consent before collection); Rule 6 (disclosure to third parties requires prior permission). These obligations remain operative alongside the DPDP Act pending formal repeal or amendment.

[23] Clinical Establishments (Registration and Regulation) Act, No. 23 of 2010, Acts of Parliament, 2010 (India) [hereinafter *CERA*]; Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, Reg. 2.2; Medical Council of India, Telemedicine Practice Guidelines, 2020.

[24] Medical Devices Rules, 2017, Rule 2(1)(h) (India) [hereinafter *Medical Devices Rules*] (defining software as a medical device to include software intended for diagnosis or treatment); CENTRAL DRUGS STANDARD CONTROL ORGANISATION, REGULATORY GUIDELINES FOR SOFTWARE AS MEDICAL DEVICE (Jan. 2022) [hereinafter *CDSCO SaMD Guidelines*] (Class A to D risk classification; Class C and D require conformity assessment and clinical investigation prior to market authorisation).

 [ISSN 2581-5369]

ABHA ecosystem.[2526] The ABDM Policy prohibits secondary use of health records without fresh, granular consent and requires Health Information Providers and Health Information Users to register with the National Health Authority and comply with data governance standards. However, these are administrative policies rather than enforceable statutes, and their intersection with the DPDP Act's consent framework has not been judicially resolved.

E. Consumer Protection and Medical Negligence

Under the Consumer Protection Act, 2019, patients are 'consumers' of healthcare services, and hospitals are liable for 'deficiency in service,' including negligent clinical care.[27] The Supreme Court's landmark rulings in *Jacob Mathew v. State of Punjab*,[28] *Spring Meadows Hospital v. Harjol Ahluwalia*,[29] and *V. Kishan Rao v. Nikhil Super Speciality Hospital*[30] establish that hospitals and individual practitioners are liable for negligent medical care. The central unresolved question for AI diagnostics is liability allocation when the AI system, rather than the treating physician, produces the deficient diagnosis: whether liability rests with the AI developer, the deploying hospital, or the prescribing clinician.

IV. CONSTITUTIONAL DIMENSIONS: PRIVACY, EQUALITY, AND BODILY AUTONOMY

A. Article 21: The Right to Informational Privacy and Bodily Autonomy

The Supreme Court in *Puttaswamy I* recognised that the right to privacy encompasses multiple dimensions, including informational privacy, the right to control the collection, retention, and use of personal information, and decisional privacy, the right to make personal decisions without

[25] *ABDM Policy*, *supra* note 9.
[26] NATIONAL DIGITAL HEALTH BLUEPRINT, MINISTRY OF HEALTH & FAMILY WELFARE (2019) [hereinafter *NDHB*] (articulating privacy by design, data sovereignty, and consent-based interoperability); NATIONAL HEALTH POLICY, 2017 (recognising protection of patient data as ancillary to the right to health under Article 21).
[27] Consumer Protection Act, No. 35 of 2019, § 2(7), Acts of Parliament, 2019 (India) [hereinafter *CPA 2019*]; § 2(9) (deficiency in service); § 86; *Martin F. D'Souza v. Mohd. Ishfaq*, (2009) 3 S.C.C. 1 (India) (medical negligence requires breach of a duty of care; Consumer Protection Act applies to healthcare establishments and practitioners providing services for consideration).
[28] *Jacob Mathew v. State of Punjab*, (2005) 6 S.C.C. 1 (India) (three-part test for medical negligence: duty of care, breach, and resulting damage; an error of judgment is not per se negligence, but a gross and culpable departure from accepted practice is); *Vinitha Ashok v. Lakshmi Hospital*, (2001) 8 S.C.C. 731 (India) (applying the Bolam standard).
[29] *Spring Meadows Hospital v. Harjol Ahluwalia*, (1998) 4 S.C.C. 39 (India) (hospitals liable under the Consumer Protection Act for deficiency of service caused by medical negligence; institutional liability where hospital systems are defective).
[30] *V. Kishan Rao v. Nikhil Super Speciality Hospital*, (2010) 5 S.C.C. 513 (India) (Consumer Forum competent to adjudicate medical negligence; expert evidence necessary but not mandatory in all cases; where facts clearly demonstrate negligence, the forum may draw an inference without expert testimony).

 [ISSN 2581-5369]

state interference.[31] Both dimensions are directly engaged by the secondary use of patient health data for AI training. Informational privacy is violated when health data shared in the intimacy and trust of the clinical encounter is processed for commercial AI development without the patient's informed and specific consent. Decisional privacy is violated when an AI system, trained on data whose parameters the patient could not influence, generates a clinical determination that shapes their treatment pathway without adequate transparency, explanation, or opportunity for contestation.

The *Selvi v. State of Karnataka* judgment, holding that bodily and informational integrity cannot be accessed by the state absent voluntary consent, extends by analogy to the compelled sharing of health data for AI system training: where consent is obtained through standard forms that do not specifically disclose AI training purposes, the consent is not voluntary in the constitutionally meaningful sense.[32] The chilling-effect doctrine, articulated in *Shreya Singhal v. Union of India*,[33] provides a further constitutional constraint: legal frameworks that deter patients from seeking medical care or from honestly disclosing symptoms due to fears about secondary commercial use of their health data violate Article 19 by chilling the exercise of personal autonomy in healthcare.

B. Article 14: Equality and the Problem of Algorithmic Discrimination

Algorithmic bias in AI diagnostic systems raises acute Article 14 concerns. AI diagnostic tools trained on health datasets that under-represent women, lower-income populations, and minority communities produce systematic diagnostic errors for these groups, a form of technological discrimination that is facially neutral but structurally unequal. Buolamwini and Gebru's foundational study documented error rates up to 34.7 per cent for darker-skinned women in automated classification systems trained on non-representative datasets.[34] Applied to diagnostic AI, such bias translates directly into missed diagnoses, delayed treatment, and worse health outcomes for already-marginalised populations.

---

[31] *Puttaswamy I*, *supra* note 13, ¶¶ 180–85 (proportionality requires a law, a legitimate aim, necessity, and proportionality *stricto sensu*); *Modern Dental College v. State of M.P.*, (2016) 7 S.C.C. 353 (India) (adopting the four-stage proportionality analysis).

[32] *Selvi v. State of Karnataka*, (2010) 7 S.C.C. 263 (India) (compelled narco-analysis and polygraph examinations violate the Article 20(3) privilege; bodily and informational integrity cannot be accessed by the state without informed, voluntary consent).

[33] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India) (laws governing digital spaces must satisfy strict proportionality review; a chilling effect on fundamental rights renders overbroad regulation constitutionally infirm).

[34] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 1, 7–9 (2018) (error rates up to 34.7% for darker-skinned women compared to 0.8% for lighter-skinned men; first systematic demonstration of intersectional algorithmic bias).

 [ISSN 2581-5369]

Under the transformative constitutionalism articulated in *Navtej Singh Johar v. Union of India*, and applicable to entities exercising public functions including large hospitals and health-tech platforms, AI systems that reproduce structural discrimination against marginalised groups may constitute a violation of Article 14 even in the absence of discriminatory intent.[35] The failure to require demographic bias testing and performance disaggregation as conditions of AI diagnostic deployment is therefore not merely a regulatory oversight; it is a potential constitutional failure.

V. COMPARATIVE LEGAL ANALYSIS: EU AND UNITED STATES FRAMEWORKS

A. The European Union: An Integrated Regulatory Architecture

The EU has constructed the world's most advanced integrated regulatory architecture for AI-driven health data governance, through the interaction of the GDPR, the EU AI Act, and the European Health Data Space (EHDS) Regulation.

Under GDPR Article 9, health data is a 'special category' attracting the highest level of protection under EU data protection law.[36] Processing is prohibited unless an express exception applies: explicit consent under art. 9(2)(a); healthcare purposes under art. 9(2)(h); scientific research under art. 9(2)(j); or substantial public interest under art. 9(2)(g). Secondary use of health data for AI training typically requires either explicit, research-specific consent or a sufficiently specific national research exemption enacted by statute, the CJEU having held in Case C-34/21 that generic national research exceptions without specific content do not satisfy the GDPR's 'more specific' requirement.[37] GDPR Article 22 provides patients the right not to be subject to solely automated decisions with significant effects on them, a right directly applicable to AI diagnostic systems and algorithmic coverage determinations.

The EU AI Act classifies AI systems used for medical diagnosis, AI-assisted treatment decisions, and health-insurance profiling as 'high-risk,'[38] requiring mandatory fundamental rights impact assessments, transparency and explainability obligations, human oversight

[35] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 234–37 (India) (transformative constitutionalism under Article 14; state action or systems that reproduce structural discrimination may violate the equality guarantee even absent discriminatory intent).

[36] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 9, 2016 O.J. (L 119) 1 [hereinafter *GDPR*] (prohibition on processing special categories of personal data, including health data, subject to exceptions including explicit consent (art. 9(2)(a)), healthcare purposes (art. 9(2)(h)), scientific research (art. 9(2)(j)), and substantial public interest (art. 9(2)(g))); art. 22 (right not to be subject to solely automated decisions); art. 35 (data protection impact assessments).

[37] Irene Moulitsas et al., *EU GDPR and Secondary Use of Health and Genetic Data for Research Support Purposes*, INT'L DATA PRIVACY L. (Jan. 28, 2026); Case C-34/21 (C.J.E.U.) (national research exemptions must have specific content distinct from the general rules of the GDPR).

[38] Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), Annex III, ¶ 5(a)–(d), 2024 O.J. (L 1689) 1 [hereinafter *EU AI Act*] (classifying AI systems for medical diagnosis, treatment, and health-insurance profiling as high-risk, requiring conformity assessment, fundamental rights impact assessment, technical documentation, and EU database registration before market placement).

 [ISSN 2581-5369]

requirements, and EU-wide database registration before market placement. Article 10(5) permits processing of health data for AI bias detection under strict conditions, creating a structured pathway for secondary use of sensitive health data that the Indian framework lacks.[39]

The EHDS Regulation, which entered into force on March 26, 2025, creates the world's first structured framework for cross-border secondary use of health data, including for AI development and clinical research.[40] It establishes Health Data Access Bodies in each member state to receive and process data-access applications; specifies permissible secondary-use purposes; mandates pseudonymisation as a technical safeguard; and prohibits re-identification. The EHDS' interaction with the GDPR's purpose-limitation principle, particularly whether AI training on secondary health data constitutes 'compatible' further processing, remains under active regulatory clarification.[41]

B. The United States: Constitutional and HIPAA Frameworks

The United States' regulatory framework for healthcare AI data privacy rests primarily on HIPAA's Privacy, Security, and Breach Notification Rules, supplemented by the FTC Act and state privacy statutes.[42] The US Department of Health and Human Services' Office for Civil Rights proposed, on January 6, 2025, the first major update to the HIPAA Security Rule in twenty years, explicitly addressing AI-related cyber security obligations for covered entities and business associates holding electronic protected health information.

OCR's 2025 HIPAA enforcement record was the second-highest annual count on record: 21 financial-penalty resolutions collecting $8,330,066, with AI-related incidents explicitly identified as an emerging enforcement priority.[43] Significant 2025 enforcement actions included

[39] *EU AI Act*, *supra* note 38, art. 10(5) (processing of sensitive data strictly necessary for bias detection and correction, subject to safeguards); art. 13 (transparency); art. 14 (human oversight).
[40] Regulation 2025/327, of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space, arts. 33–50, 2025 O.J. (L 327) 1 [hereinafter *EHDS Regulation*] (secondary-use framework: Health Data Access Bodies adjudicate access applications; data permits specify permissible purposes, pseudonymisation, and prohibition on re-identification); art. 41 (data holders must make data available within specified timelines). The Regulation entered into force on March 26, 2025.
[41] ATLANTIC COUNCIL, NAVIGATING THE EUROPEAN UNION'S AI AND HEALTH DATA FRAMEWORK 8–10 (Apr. 2026) (documenting the tension between the Commission's push for greater data sharing for AI innovation and member states' stricter interpretations of GDPR special-category protections).
[42] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [hereinafter *HIPAA*]; 45 C.F.R. pts. 160, 162, 164 (2024) (Privacy, Security, and Breach Notification Rules); U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Security Rule Updates: Proposed Rule (Jan. 6, 2025) (first major Security Rule revision in twenty years, with enhanced AI-related cybersecurity obligations).
[43] U.S. Dep't of Health & Human Servs., Office for Civil Rights, HIPAA Enforcement: 2025 Year in Review (Dec. 2025) [hereinafter *OCR 2025 Report*] (21 financial penalty resolutions collecting $8,330,066 in 2025, the second-highest annual count on record; AI-related incidents identified as an emerging enforcement priority).

 [ISSN 2581-5369]

settlements with Cadia Healthcare Facilities ($182,000),[44] Vision Upright MRI, BayCare Health System, and Comstar LLC for failures in risk analysis, breach notification, and access controls. AI is now explicitly on OCR's enforcement radar, with the agency warning that a single misconfigured inference endpoint with access to live electronic health record data represents potential exposure of thousands of patient records per hour.

The UK's Data (Use and Access) Act 2025 provides a further comparative reference: it establishes information standards for health and social care data systems relevant to AI-driven secondary use and creates the Information Commission as the successor to the ICO, with expanded powers.[45]

VI. LATEST CASE LAW AND LEGAL DEVELOPMENTS

A. Estate of Gene B. Lokken v. UnitedHealth Group, Inc. (D. Minn. 2025 to 2026)

The most significant pending case in global healthcare AI liability is *Lokken v. UnitedHealth Group*, a class action filed in November 2023 and currently advancing in the United States District Court for the District of Minnesota.[46] UnitedHealth's nH Predict AI model, trained on six million patients' historical data, was alleged to deny Medicare Advantage members post-acute care coverage by overriding treating physicians' recommendations and predicting the moment when UnitedHealth would cut payment for care, regardless of actual medical need. The plaintiffs' complaint alleged that UnitedHealth was aware that the nH Predict model had a 90 per cent error rate, demonstrated by the fact that over 90 per cent of denied claims were overturned on internal appeal or before federal administrative law judges, but continued to use the model because only approximately 0.2 per cent of denied patients actually completed the appeal process.[47]

On February 13, 2025, the court granted in part and denied in part UnitedHealth's motion to dismiss, allowing the breach of contract and breach of implied covenant of good faith and fair dealing claims to proceed.[48] The court found that the Medicare Act did not preempt claims challenging the use of AI as a gatekeeper where plan documents had promised physician-led

[44] HHS Office for Civil Rights, Cadia Healthcare Facilities Resolution Agreement and Corrective Action Plan (Sept. 30, 2025) ($182,000 settlement; two-year corrective action plan following impermissible disclosure of protected health information).
[45] Data (Use and Access) Act 2025, c. 32 (UK) (establishing information standards for health and social care data systems; creating the Information Commission as successor to the Information Commissioner's Office).
[46] *Lokken*, *supra* note 3.
[47] *Lokken*, *supra* note 3 (plaintiffs alleging that nH Predict, trained on a database of six million patients, was used to override physician determinations; more than 90% of denied claims overturned on appeal; as of April 2026 the magistrate judge ordered production of tens of thousands of AI-related documents by April 29, 2026).
[48] *Lokken*, *supra* note 3 (discovery proceedings; April 2026 document-production order).

 [ISSN 2581-5369]

medical review. As of April 2026, Magistrate Judge Shannon G. Elkins ordered UnitedHealth to produce tens of thousands of AI-related documents to plaintiffs by April 29, 2026. The case establishes two foundational legal principles with global significance: first, that AI-driven clinical decisions must honour contractual commitments to physician-led review; and second, that continued use of a demonstrably inaccurate AI model, when the deploying organisation is aware of its error rate and the vulnerability of those affected, may satisfy the knowledge element for bad faith liability.

B. Sutter Health & Me v. Doe (N.D. Cal. 2026)

In *Sutter Health & Me v. Doe*, a class action filed in April 2026 in the Northern District of California, plaintiffs allege that two major California healthcare organisations deployed an AI clinical documentation tool that recorded patient-clinician conversations without patients' knowledge or consent, transmitting audio files to third-party servers for processing and transcription.[49] The case alleges violations of the federal Wiretap Act and the California Confidentiality of Medical Information Act (CMIA), and raises the question of whether using an AI tool, even one that improves clinical documentation efficiency, constitutes a waiver of the physician-patient privilege and a violation of HIPAA's minimum-necessary standard when the recordings are transmitted to a vendor beyond the covered entity's control.

C. German Federal Court of Justice on GDPR Article 9 Health Data

The German Federal Court of Justice, in its judgment of October 14, 2025 (VI ZR 431/24), confirmed that GDPR Article 9(1) constitutes a market conduct rule under German unfair competition law, expanding enforcement of special-category data-protection obligations beyond data protection authorities to civil litigation by private parties, including competitors.[50] This development is significant for AI health data governance: it creates a private right of action against entities that improperly process health data for AI training in violation of GDPR Article 9, beyond the administrative enforcement mechanisms of data protection supervisory authorities.

D. India: Constitutional Challenges and Pending Litigation

In India, the constitutional challenge filed by the Reporters' Collective before the Supreme Court in February 2026, contesting the DPDP Act's RTI-curtailment provisions and surveillance-enabling exemptions under Section 17,[51] provides an imminent opportunity for the

[49] *Sutter Health & Me v. Doe*, *supra* note 4.
[50] *GDPR*, *supra* note 36, art. 9; BGH, VI ZR 431/24 (Oct. 14, 2025) (Ger.).
[51] *DPDP Act*, *supra* note 5, § 17(2)–(3); *Reporters' Collective v. Union of India*, W.P. (C) No. 130/2026 (India) (pending).

 [ISSN 2581-5369]

Supreme Court to lay down the constitutional parameters of permissible state data processing, including in the healthcare context. The outcome of this litigation will determine whether India's health data governance regime is constitutionally adequate or requires fundamental legislative revision.

The ongoing challenges to the Criminal Procedure (Identification) Act, 2022 before the Delhi High Court in *Sahibe Alam v. Govt. of NCT of Delhi* (W.P. (Crl.) 672/2026), while not directly addressing health data, have the potential to lay down constitutional standards for biometric and personal data collection by the state that would apply with equal force to health data processing for AI purposes.

VII. LIABILITY ALLOCATION IN AI-DRIVEN HEALTHCARE DIAGNOSTICS

A. The Multi-Stakeholder Liability Problem

AI-driven healthcare diagnostics creates a multi-stakeholder liability ecosystem (developer, deploying hospital, prescribing clinician, and patient) in which the allocation of responsibility for diagnostic errors presents doctrinal challenges that India's existing legal frameworks are not equipped to resolve. Scholars have proposed a presumptive liability framework placing responsibility on the entity best positioned to prevent harm,[52] but no Indian statute or authoritative judicial precedent has yet addressed the specific question of who bears liability when an AI diagnostic tool produces a clinically harmful erroneous output.

Under the current Consumer Protection Act and tort framework, the hospital deploying the AI system bears primary liability for deficiency of service, since the patient's contractual relationship is with the hospital and the AI developer is a third-party vendor. *Jacob Mathew*'s three-part negligence test (duty, breach, and damage)[53] applies to AI diagnostic errors in the following manner: the hospital owes a duty of care to patients; deployment of an AI diagnostic tool known to have systematic errors or inadequate validation constitutes a breach of that duty; and a consequential misdiagnosis causing harm satisfies the damage element. The prescribing clinician who over-relies on an AI output without applying independent clinical judgment may additionally be liable for gross departure from the standard of care.

[52] I. Glenn Cohen, *Artificial Intelligence in Medicine: Mitigating Risks and Maximizing Benefits*, 1 NATURE MED. 1, 3–4 (2020) (proposing a presumptive liability framework placing responsibility on the entity best positioned to prevent harm); Nigam H. Shah et al., *Artificial Intelligence and Machine Learning in Clinical Development: A Translational Perspective*, 4 NPJ DIGITAL MED. 1, 3–5 (2019).

[53] *Jacob Mathew*, *supra* note 28 (three-part negligence standard: duty, breach, damage).

B. The 'Black Box' Problem and the Right to Explanation

A foundational challenge for liability adjudication in AI diagnostic cases is the 'black box' problem: AI systems, particularly deep learning neural networks, produce outputs through computational processes that cannot be fully explained even by their designers.[54] When a patient or consumer forum seeks to establish that an AI diagnostic tool produced a negligent output, the inability to access or explain the system's decision pathway creates a fundamental asymmetry of information, compounded by the fact that the developer holds the proprietary algorithm and typically refuses disclosure on grounds of trade secrecy.

The EU AI Act's transparency and explainability obligations under Article 13, requiring providers of high-risk AI to ensure systems are 'sufficiently transparent that deployers can understand the system's output and use it appropriately,'[55] provide a comparative model for the minimum disclosure standard required in Indian AI diagnostic liability cases. India's CDSCO AI Draft Guidance, 2025 proposes algorithmic transparency reporting as a pre-market requirement, but this requirement has not been formally enacted.[56]

VIII. TOWARDS A RIGHTS-BASED REGULATORY FRAMEWORK FOR AI HEALTH DATA IN INDIA

A. Proposed Framework: Five Pillars

Drawing upon the constitutional analysis, comparative review, and doctrinal critique above, this section proposes a five-pillar framework for India's governance of secondary use of patient data for AI diagnostics.

First, establish a special category regime for health data. Parliament must amend the DPDP Act, 2023 to designate health and medical data as a 'special category' requiring heightened protection, aligned with the EU GDPR Article 9 model and consistent with the SPDI Rules' pre-existing classification. This amendment must prohibit secondary use of health data for AI training absent explicit, purpose-specific, revocable consent, and must specify that no single consent clause in a general hospital admission form can constitute valid consent for AI training purposes. The right to erasure from AI training datasets must be made explicit and technically enforceable.[57]

[54] PASQUALE, *supra* note 10; EUBANKS, *supra* note 10.
[55] *EU AI Act*, *supra* note 38, arts. 10(5), 13–14.
[56] *CDSCO AI Draft Guidance*, *supra* note 6.
[57] *DPDP Act*, *supra* note 5; *DPDP Rules 2025*, *supra* note 16.

 [ISSN 2581-5369]

Second, enact an AI Medical Devices and Diagnostics Safety Act. The CDSCO AI Draft Guidance, 2025 must be legislatively enacted as a binding statute, incorporating mandatory pre-market conformity assessment for AI/ML-based SaMD; demographic bias testing against India-representative datasets as a condition of market authorisation; algorithmic transparency reporting accessible to deploying hospitals and patients; and continuous post-market surveillance with mandatory adverse-event reporting.[58]

Third, create a Health Data Access Authority. Modelled on the EHDS' Health Data Access Bodies, India should establish a statutory Health Data Access Authority under the Ministry of Health and Family Welfare, empowered to receive and adjudicate applications for secondary use of health data for AI research and development; specify permissible secondary-use purposes and associated safeguards; mandate pseudonymisation and federated learning architectures where technically feasible; and audit compliance by data fiduciaries holding health datasets.[59]

Fourth, codify explicit AI liability allocation. Parliament must enact specific provisions addressing liability for AI-induced diagnostic error, placing primary liability on the deploying hospital as the entity in privity of contract with the patient, secondary liability on the AI developer for inadequate validation or undisclosed known inaccuracies, and clinician liability for gross over-reliance on AI outputs without independent clinical judgment. A strict liability regime should apply where AI systems are deployed without completing mandatory pre-market conformity assessment.[60]

Fifth, establish DPDP-health sector sectoral guidelines and a phased compliance architecture. The Data Protection Board of India, once constituted under the DPDP Act, should issue sector-specific guidelines for healthcare data fiduciaries, specifying mandatory consent-management-platform requirements for AI health data processing; standard form clauses for AI-specific consent; minimum security safeguards for AI model training datasets, including encryption, access logging, and breach detection; and a phased compliance timeline consistent with the DPDP Rules' 18-month rollout framework but with healthcare-specific milestones.[61]

---

[58] *CDSCO AI Draft Guidance*, *supra* note 6 (proposing mandatory pre-market review, clinical validation, algorithmic transparency reporting, demographic bias assessment, and continuous post-market surveillance; pending formal notification).
[59] *EHDS Regulation*, *supra* note 40, arts. 33–50.
[60] *Jacob Mathew*, *supra* note 28 (gross and culpable departure from accepted medical practice constitutes actionable negligence, applicable to hospitals deploying AI diagnostic tools with known error rates).
[61] *DPDP Act*, *supra* note 5, §§ 16, 33, 40.

 [ISSN 2581-5369]

IX. CONCLUSION

AI-driven healthcare diagnostics represents one of the most promising technological developments of the twenty-first century and one of its most acute legal challenges. The same data pipeline that enables an AI system to detect early-stage lung cancer in a chest X-ray more accurately than a radiologist also enables that system to embody, reflect, and amplify the biases embedded in historically collected medical data; to generate clinical determinations from opaque computational processes that are not transparent to the physician relying upon them or the patient affected by them; and to create commercial value from patients' intimate medical histories without their informed engagement or equitable participation.[62]

India stands at a decisive regulatory moment. Its constitutional framework, grounded in the *Puttaswamy* judgments' proportionality standard and the transformative constitutionalism of Articles 14, 19, and 21, provides a robust normative foundation for rights-respecting AI health data governance. Its legislative framework, comprising the DPDP Act, 2023, the DPDP Rules, 2025, the SPDI Rules, the CERA, and the Medical Devices Rules, provides a starting architecture. Its digital health infrastructure, comprising the ABDM ecosystem, the ABHA health records, and the National Digital Health Blueprint, creates the operational substrate for a genuinely transformative data-driven healthcare system. But the gap between this foundation and the legal framework required to govern AI-driven secondary use of patient data is substantial, structural, and growing with every month that passes without legislative action.[63]

The international evidence is unambiguous. In the United States, *Lokken v. UnitedHealth Group* has established that AI healthcare systems must honour contractual commitments to physician-led review and that deploying demonstrably inaccurate AI tools with knowledge of their error rates may constitute actionable bad faith. OCR's 2025 HIPAA enforcement record demonstrates that AI-related health data incidents are now an active regulatory enforcement priority. In the European Union, the GDPR-EU AI Act-EHDS triptych has created the world's most sophisticated framework for balancing AI innovation against health data rights. Germany's Federal Court of Justice has expanded GDPR Article 9 enforcement to private litigation, creating competitive incentives for health data compliance. India cannot afford to wait for its own *Lokken* moment, for the judicial clarification of AI health liability to arrive through the

[62] Buolamwini & Gebru, *supra* note 34.
[63] *Puttaswamy I*, *supra* note 13.

 [ISSN 2581-5369]

suffering of patients harmed by AI systems deployed in the absence of an adequate legal framework.[64]

The reforms proposed in this paper, namely a special category regime for health data, an AI Medical Devices and Diagnostics Safety Act, a Health Data Access Authority, explicit AI liability codification, and sector-specific DPDP guidelines, are not aspirational. They respond to operative constitutional obligations, to live legislative lacunae, and to a healthcare AI deployment reality that is already generating patient harm in the absence of regulatory constraint. A constitutional democracy that recognises privacy as a fundamental right, that has built a digital health infrastructure promising universal access to quality care, and that has committed itself to the rule of law cannot permit the most intimate data generated by its citizens' bodies to be processed for commercial AI development without their informed consent, without transparency, without accountability, and without an adequate legal remedy when that processing harms them. The constitutional framework requires more. India's patients deserve more.[65]

X. RECOMMENDATIONS

A. Legislative Recommendations

Amend the DPDP Act, 2023 to designate health and medical data as a special category requiring heightened protection, with explicit prohibition on secondary use for AI training absent purpose-specific, revocable, informed consent; a mandatory right to erasure from AI training datasets; and removal of the Section 17 exemptions for state health data processing that fail the *Puttaswamy* proportionality test.[66]

Enact an AI Medical Devices and Diagnostics Safety Act translating the CDSCO AI Draft Guidance, 2025 into binding statute, incorporating mandatory pre-market conformity assessment, demographic bias testing, algorithmic transparency reporting, and continuous post-market surveillance with adverse-event reporting for AI/ML-based SaMD.[67]

Establish a statutory Health Data Access Authority under the Ministry of Health and Family Welfare, modelled on the EU EHDS' Health Data Access Body architecture, with powers to adjudicate secondary-use applications, specify permissible purposes and safeguards, mandate privacy-enhancing technologies, and audit compliance.[68]

---

[64] *Lokken*, *supra* note 3.
[65] *DPDP Act*, *supra* note 5; *DPDP Rules 2025*, *supra* note 16.
[66] *DPDP Act*, *supra* note 5; *DPDP Rules 2025*, *supra* note 16.
[67] *Medical Devices Rules*, *supra* note 24, Rule 2(1)(h); *CDSCO SaMD Guidelines*, *supra* note 24.
[68] *EHDS Regulation*, *supra* note 40, arts. 33–50.

 [ISSN 2581-5369]

Enact explicit AI liability allocation provisions within the Consumer Protection Act, 2019 or through standalone legislation, placing primary liability on deploying hospitals, secondary liability on AI developers for inadequate validation or undisclosed known inaccuracies, and clinician liability for gross over-reliance, with strict liability where mandatory pre-market requirements have not been completed.[69]

Amend the Ayushman Bharat Digital Mission Health Data Management Policy, 2023 to accord it statutory rather than administrative status, and update its consent framework to explicitly address AI training as a category of secondary use requiring fresh, granular, purpose-specific consent beyond the clinical consent obtained at the point of care.[70]

B. Judicial Recommendations

Constitutional standards for state health data processing. The Supreme Court, in adjudicating the Reporters' Collective challenge to the DPDP Act, should lay down constitutional standards for state health data processing, including by public hospitals and the National Health Authority, that satisfy the *Puttaswamy* proportionality framework and cannot be displaced by Section 17 executive orders.[71]

A rebuttable presumption of deficiency in service. Consumer courts adjudicating AI diagnostic liability claims should adopt a rebuttable presumption of deficiency in service where an AI diagnostic system was deployed without completing mandatory medical-device registration or conformity assessment; the system was known to have systematic error rates above clinically acceptable thresholds; or the deploying hospital is unable to produce audit trails demonstrating human oversight of AI outputs.[72]

C. Institutional Recommendations

Healthcare-specific sectoral guidelines. The Data Protection Board of India, once constituted under the DPDP Act, should issue healthcare-specific sectoral guidelines within six months of constitution, specifying consent-management-platform requirements, AI training data governance standards, minimum security safeguards, and a phased compliance timeline with healthcare-specific milestones.[73]

---

[69] *CPA 2019*, *supra* note 27, §§ 2(7), (9), 86; *Martin F. D'Souza*, *supra* note 27.
[70] *ABDM Policy*, *supra* note 9.
[71] *DPDP Act*, *supra* note 5, § 17(2)–(3); *Reporters' Collective v. Union of India*, W.P. (C) No. 130/2026 (India) (pending).
[72] *CPA 2019*, *supra* note 27, §§ 2(7), (9).
[73] *DPDP Act*, *supra* note 5, §§ 16, 33.

 [ISSN 2581-5369]

Formal notification of the AI Draft Guidance. The Central Drugs Standard Control Organisation should formally notify the AI Draft Guidance, 2025 as binding regulations without further delay, and establish a dedicated AI Medical Devices Division with technical capacity to conduct conformity assessments and adverse-event investigations for AI diagnostic software.[74]

Participation in the European Health Data Space. India should actively participate in the governance framework of the European Health Data Space and in bilateral data cooperation with EU member states, to ensure that Indian patients' health data exported for AI research benefits from the EHDS' secondary-use safeguards and that Indian AI diagnostic developers gain access to quality European health datasets under appropriate governance conditions.[75][76]

*****

[74] *CDSCO AI Draft Guidance*, *supra* note 6.
[75] *EHDS Regulation*, *supra* note 40.
[76] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225 (2024) [hereinafter *CoE AI Convention*]; G.A. Res. 78/265, Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (Mar. 21, 2024).

 [ISSN 2581-5369]