RESEARCH PAPER

Right To Health In The Era Of Artificial Intelligence: Examining Regulatory Gaps In India's Digital Health Governance Framework

Rishi Bhargava*[1], Vishesh Dahiya[2], Saif Hussain[3], Akshay Garg[4], Prof. (Dr.) Birendra Kumar Tiwari[5]

[1] *Assistant Professor, School of Law, SVKM's NMIMS (deemed to be university) Indore Campus; rishibhargava.research@gmail.com
[2]. Assistant Professor, Faculty of Law, Jagran Lakecity University, Bhopal (M.P.)
[3]. Assistant Professor, Faculty of Law, Jagran Lakecity University, Bhopal (M.P.)
[4]. Assistant Professor, School of Law, SVKM's NMIMS (deemed to be university) Indore Campus
[5]. Professor, Technocrats Institute of Law, Affiliated to Barkatullah University, Bhopal (M.P.)

***Corresponding author:** Rishi Bhargava, rishibhargava.research@gmail.com

Abstract
The rapid integration of Artificial Intelligence (AI) into healthcare delivery, clinical diagnostics, drug regulation, insurance underwriting, and public health surveillance has fundamentally altered the landscape of health governance in India. While AI promises transformative improvements in healthcare access—particularly in a country burdened by a physician-to-patient ratio of 1:834 against the WHO-recommended 1:1000—its deployment in health systems raises acute legal and constitutional concerns that India's existing regulatory architecture is ill-equipped to address. This paper critically examines the intersection of the constitutional right to health, as evolved through Articles 21 and 47 of the Indian Constitution, with the emerging phenomenon of AI-driven digital health governance. It analyses specific regulatory gaps in the Ayushman Bharat Digital Health Mission (ABDM), the Digital Personal Data Protection Act, 2023, and the proposed amendments to the Drugs and Cosmetics Act, 1940, arguing that algorithmic opacity, absence of explainability mandates, discriminatory data bias, and inadequate liability frameworks together constitute a structural threat to the justiciability of the right to health. Drawing from the European Union Artificial Intelligence Act, 2024, and the United States Food and Drug Administration's approach to AI-enabled Software as a Medical Device (SaMD), the paper proposes a rights-centric legislative framework for AI governance in Indian healthcare, rooted in constitutional morality, informed consent, algorithmic accountability, and equitable digital health infrastructure. The paper adopts a doctrinal and comparative methodology.

Keywords: Right to Health, Artificial Intelligence, Digital Health Governance, ABDM, Algorithmic Accountability, DPDP Act 2023, Software as Medical Device, Constitutional Law, India.
How to cite this article: Bhargava R, Dahiya V, Hussain S, Garg A, Tiwari BK. Right To Health In The Era Of Artificial Intelligence: Examining Regulatory Gaps In India's Digital Health Governance Framework. Int J Drug Deliv Technol. 2026;16(5): 1328-1335. DOI: 10.25258/ijddt.16.5.122

1. Introduction

India stands at a critical inflection point in health governance. The Ayushman Bharat Digital Health Mission (ABDM), launched in 2021 and operationalised through the National Health Authority, envisions a unified digital health ecosystem nchored in Artificial Intelligence (AI), big data analytics, and interoperable electronic health records.[1] India's AI-in-healthcare market, valued at approximately USD 1.7 billion in 2023, is projected to grow at a compound annual growth rate (CAGR) of 40.8 per cent through 2030.[2] Simultaneously, AI-driven diagnostic tools, algorithmic triage systems, AI-assisted drug discovery platforms, and machine-learning-based insurance eligibility assessors are being deployed across public and private healthcare settings without a coherent overarching legal framework. The Indian Supreme Court, in a long line of decisions beginning with *Paschim Banga Khet Mazdoor Samity v. State of West Bengal*,[3] has held that the right to life under Article 21 of the Constitution encompasses the right to health and emergency medical care. Article 47 imposes a directive duty upon the State to improve public health. The deployment of AI in healthcare is, therefore, not merely a technological policy choice—it is a constitutional question that demands rigorous legal scrutiny.

[1]Ministry of Health and Family Welfare, Government of India, "Ayushman Bharat Digital Health Mission: Operational Guidelines" (National Health Authority, 2022), available at https://abdm.gov.in.

[2]Grand View Research, "India Artificial Intelligence in Healthcare Market Size Report 2024" (2024), available at https://www.grandviewresearch.com (last visited Apr. 5, 2025).

[3]Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37 (India).

*Author for Correspondence: rishibhargava.research@gmail.com

The legal concern is multi-layered. First, AI systems in healthcare are frequently opaque: their diagnostic or eligibility-determination outputs cannot be explained in comprehensible terms, directly threatening the principle of informed consent established in *Samira Kohli v. Dr. Prabha Manchanda*.[4] Second, AI systems trained on datasets that under-represent women, rural populations, and marginalised communities risk amplifying existing health inequalities, in possible violation of Articles 14 and 15.[5] Third, India's existing regulatory framework—the Drugs and Cosmetics Act, 1940, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 (DPDP Act)—does not adequately address the risks posed by AI as a healthcare decision-making instrument.

This paper proceeds as follows. Section 2 maps AI deployment in Indian healthcare. Section 3 analyses constitutional foundations of the right to health and their application to AI-driven health governance. Section 4 identifies specific regulatory gaps. Section 5 surveys comparative regulatory models from the European Union and the United States. Section 6 proposes a rights-centric legislative framework. Section 7 concludes.

2. Artificial Intelligence in Indian Healthcare: Landscape and Deployment

The deployment of AI in Indian healthcare spans five primary domains: clinical diagnostics, drug discovery and regulation, health insurance underwriting, public health surveillance, and telemedicine. Each domain presents distinct governance challenges.

In clinical diagnostics, AI-powered tools are deployed for radiology interpretation, pathology screening, and ophthalmic disease detection. AIIMS New Delhi has piloted AI-based diabetic retinopathy screening systems, and the National Cancer Grid has explored AI for histopathological cancer diagnosis.[6] The Niramai Health Analytix platform uses thermal imaging and machine learning for early breast cancer screening—significant given India's low mammography penetration in rural areas.[7]

In drug regulation, AI platforms are leveraged to identify therapeutic candidates and predict drug-protein interactions. The Central Drugs Standard Control Organisation (CDSCO) has acknowledged AI-assisted submissions under the New Drugs and Clinical Trials Rules, 2019,[8] though no formal statutory regulatory pathway exists for AI-generated pharmacological evidence. The CDSCO issued a Draft Guidance Document on AI/ML-Based Software as a Medical Device in 2024,[9] which, being a non-binding administrative document, creates no enforceable obligations for developers or deployers.

Health insurance underwriting increasingly employs AI algorithms to assess risk profiles, determine premium structures, and adjudicate claims. The Insurance Regulatory and Development Authority of India (IRDAI) in its 2024 Insurance Products Regulations acknowledges AI-based underwriting[10] but stops short of mandating explainability or non-discrimination standards. Public health surveillance received a significant AI boost during the COVID-19 pandemic through the Aarogya Setu contact tracing application,[11] which raised unresolved concerns about mass surveillance, data retention, and absence of a statutory basis for its operation.

Finally, telemedicine—accorded legislative recognition through the Telemedicine Practice Guidelines, 2020[12]—increasingly interfaces with AI-assisted diagnostic support tools. The Guidelines are, however, entirely silent on the standards applicable when clinical advice is partly generated or supported by AI systems, creating a normative vacuum at the interface of medical ethics and algorithmic decision-making.

3. Constitutional Foundations: Right to Health and AI Governance

3.1 The Right to Health Under Article 21

The Indian Constitution does not expressly enumerate the right to health as a fundamental right. However, a robust jurisprudential tradition has located it within the right to life and personal liberty under Article 21. In *Consumer Education and Research Centre v. Union of India,* the Supreme Court declared that the right to health

[4]Samira Kohli v. Dr. Prabha Manchanda, (2008) 2 SCC 1 (India) (holding that informed consent is an essential component of the patient's right under Article 21).

[5]Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447-453.

[6]National Cancer Grid, "Annual Report 2022-23" (Tata Memorial Centre, 2023). See also Gulshan V, et al., "Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs," 316 JAMA 2402 (2016).

[7]Niramai Health Analytix, "Thermalytix: A Non-Contact, Non-Invasive Radiation-Free Breast Screening Solution" (2023), available at https://www.niramai.com (last visited Apr. 4, 2025).

[8]New Drugs and Clinical Trials Rules, 2019, G.S.R. 227(E), Ministry of Health and Family Welfare, Government of India (2019).

[9]Central Drugs Standard Control Organisation, "Guidance Document on Artificial Intelligence and Machine Learning-Based Software as Medical Devices" (Draft, 2024) (India).

[10]Insurance Regulatory and Development Authority of India, "IRDAI (Insurance Products) Regulations, 2024" (India).

[11]Sharma T, et al. Aarogya Setu: India's COVID-19 contact tracing application—a legal and privacy analysis. Journal of Law and the Biosciences. 2021;8(1):lsab017. DOI: 10.1093/jlb/lsab017.

[12]Medical Council of India, "Telemedicine Practice Guidelines, 2020," Gazette of India Extraordinary (Mar. 25, 2020), Part III, Section 4.

is an integral facet of a meaningful right to life.[13] In *Paschim Banga Khet Mazdoor Samity,* the Court imposed a positive obligation upon the State to provide emergency medical care, holding that failure constituted a violation of Article 21.[14] This positive dimension is critical: it imposes not merely a negative duty to refrain from interference, but an affirmative obligation to create and maintain accessible, equitable, and effective healthcare systems.

When the State deploys AI in healthcare—for triage, diagnosis, eligibility determination, or drug regulation—it exercises its positive obligation under Article 21. The constitutional question is whether that exercise complies with the standards of procedural fairness, non-arbitrariness, and proportionality that Article 21, read through the lens of constitutional morality articulated by Justice Chandrachud in *Puttaswamy,*[15] demands. Unaccountable AI governance does not meet this standard.

3.2 Algorithmic Opacity and the Right to Informed Consent

Informed consent is a well-established component of the right to health in Indian law. In *Samira Kohli,* the Supreme Court held that a doctor must provide the patient with adequate information concerning the nature, risks, alternatives, and consequences of a medical procedure to enable an autonomous decision.[16] Where AI systems determine diagnostic or treatment recommendations, the question arises whether meaningful informed consent can be obtained if neither the treating physician nor the patient can understand how the AI arrived at its recommendation—the "black box" problem.[17]

Contemporary deep-learning diagnostic systems, including convolutional neural networks used in radiology AI, cannot provide rule-based explanations for their outputs. The absence of a statutory explainability mandate in any current Indian health legislation means that patients may receive AI-influenced diagnoses without meaningful disclosure. This violates the constitutional standard of "just, fair, and reasonable" procedure required by Article 21 as interpreted in *Maneka Gandhi v. Union of India.*[18]

3.3 Discriminatory Bias, Article 14, and the Equality Dimension

Article 14 of the Constitution guarantees equality before the law and prohibits not only direct discrimination but also arbitrary and irrational state action.[19] Algorithmic systems in healthcare present a distinctive equality risk: they may embed and amplify existing social inequalities by perpetuating biases present in historical health data. The landmark 2019 study by Obermeyer et al. in *Science* demonstrated that a widely-deployed healthcare risk-scoring algorithm systematically underestimated the health needs of Black patients by approximately 80 per cent, because it used healthcare costs—themselves shaped by historical inequalities—as a proxy for health needs.[20] Analogous dynamics are directly plausible in the Indian context, where AI systems trained predominantly on urban, upper-income patient data may systematically underserve rural populations, women, Scheduled Castes, Scheduled Tribes, and persons with disabilities.

In the absence of mandatory algorithmic bias auditing, dataset representativeness requirements, or health impact assessments prior to AI deployment, algorithmic discrimination in Indian healthcare may proceed undetected and unchallenged. This renders the constitutional guarantee of equality under Article 14 practically illusory for those most dependent on public health systems—directly contrary to the anti-arbitrariness standard confirmed in *Ajay Hasia v. Khalid Mujib Sehravardi.*[21]

3.4 Privacy, Data Sovereignty, and the Puttaswamy Framework

The nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* unanimously recognised privacy as a fundamental right under Articles 14, 19, and 21 of the Constitution.[22] The Court articulated a tripartite test for permissible infringement: the action must be authorised by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued. Health data is among the most sensitive categories of personal information, engaging privacy interests at their most intense.

The DPDP Act, 2023 classifies health data as "sensitive personal data" requiring "explicit consent" for

[13]Consumer Education and Research Centre v. Union of India, (1995) 3 SCC 42, para 24 (India).

[14]Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37, para 9 (India).

[15]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, paras 309-315 (India) (Chandrachud, J., concurring).

[16]Samira Kohli v. Dr. Prabha Manchanda, (2008) 2 SCC 1, paras 22-28 (India).

[17]Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press; 2015. pp 3-18.

[18]Maneka Gandhi v. Union of India, (1978) 1 SCC 248, paras 56-62 (India).

[19]E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3, para 85 (India).

[20]Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447-453. DOI: 10.1126/science.aax2342.

[21]Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722, paras 741-742 (India).

[22]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

processing.[23] However, the Act's broad exemptions for state processing in the interest of national security, public order, and prevention of offences under Section 17 effectively hollow out privacy protections in the public health AI context.[24] Furthermore, Section 17(2) permits the Central Government to exempt any instrumentality of the State from all provisions of the Act—a power that, if applied to the ABDM or state health AI systems, would render the constitutional privacy guarantee unenforceable in precisely the domain where data vulnerabilities are most acute.

4. Regulatory Gaps in India's Digital Health Governance Architecture

4.1 Absence of a Regulatory Pathway for AI as Medical Device

The most fundamental regulatory gap is the absence of a statutory definition and regulated pathway for AI-enabled Software as a Medical Device (AI-SaMD). The Drugs and Cosmetics Act, 1940 and the Medical Devices Rules, 2017 (as amended in 2020) do not comprehensively address AI or software-based medical devices.[25] The CDSCO's 2024 Draft Guidance, while a welcome development, is a non-binding administrative instrument: it creates no enforceable obligations, no liability consequences for non-compliance, and no basis for judicial review. Contrast this with the EU Medical Devices Regulation (MDR) 2017/745, which provides a legally binding CE-marking pathway for AI-enabled devices with defined conformity assessment procedures, post-market surveillance obligations, and serious incident reporting requirements.[26]

4.2 No Explainability Mandate or Algorithmic Audit Requirement

Indian health law contains no statutory requirement that AI systems deployed in clinical or administrative healthcare decisions be explainable, auditable, or transparent in their operation. The DPDP Act, 2023 does not incorporate a right to explanation for automated decisions—in sharp contrast with the European General Data Protection Regulation (GDPR), Article 22 of which provides data subjects with the right not to be subject to solely automated decisions that significantly affect them, and a right to obtain a meaningful explanation.[27] The Personal Data Protection Bill, 2019—the predecessor to the DPDP Act—had contained a provision in Clause 19 granting data principals the right to explanation for significant automated decisions.[28] The omission of this provision from the enacted 2023 statute leaves a critical accountability gap in healthcare AI governance.

4.3 Liability Attribution in AI-Assisted Clinical Negligence

When an AI diagnostic system produces an erroneous recommendation that a physician relies upon to the patient's detriment, attribution of liability is deeply uncertain under existing Indian law. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 impose professional duties of care upon registered medical practitioners but make no provision for clinical errors attributable, in whole or in part, to an AI system.[29] Under the Bolam test for medical negligence as adopted by the Supreme Court in *Jacob Mathew v. State of Punjab,*[30] liability requires establishing that the treating professional departed from the standard of a reasonably competent medical professional in the field. When the impugned decision was influenced by an AI system, it is unclear whether the physician, the AI developer, the deploying hospital, or the State bears responsibility—a multiplicity of potential defendants that, combined with the difficulty of proving causation through an opaque algorithmic chain, may effectively deny patients legal remedies in violation of Articles 32 and 226 of the Constitution.

4.4 Data Governance Gaps in the ABDM Ecosystem

The ABDM operates through a federated architecture in which health data is stored across multiple Health Information Providers (HIPs) and accessed by Health Information Users (HIUs) via consent artefacts.[31] While the consent architecture is procedurally sophisticated, critical governance gaps persist. First, the ABDM consent framework permits purpose limitation to be defined broadly, potentially enabling secondary use of health data for AI training without adequate patient disclosure. Second, there is no independent oversight body with domain-specific health AI expertise; the Data Protection Board envisaged under the DPDP Act is a general-purpose complaints resolution mechanism that

[23]Digital Personal Data Protection Act, 2023, ss 2(t), 4(1)(a), 7 (India).

[24]Digital Personal Data Protection Act, 2023, s 17 (India) (providing sweeping exemptions for Government processing of data).

[25]Medical Devices Rules, 2017, S.O. 2739(E), Ministry of Health and Family Welfare, Government of India (2017), as amended by Medical Devices (Amendment) Rules, 2020.

[26]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, 2017 O.J. (L 117), arts 10, 61-82, 87.

[27]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), art 22 (2016 O.J. (L 119) 1).

[28]Personal Data Protection Bill, 2019, cl 19, Bill No. 373-C, Lok Sabha (India) (lapsed in 2022).

[29]Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, reg 1.4, Gazette of India (Apr. 11, 2002) (India).

[30]Jacob Mathew v. State of Punjab, (2005) 6 SCC 1 (India).

[31]National Health Authority, "ABDM Health Data Management Policy" (2022) (India), available at https://abdm.gov.in.

lacks specialised health AI jurisdiction and technical capacity.[32]

5. Comparative Regulatory Models: European Union and United States

5.1 The European Union Artificial Intelligence Act, 2024

The EU Artificial Intelligence Act (AI Act), adopted on 13 June 2024, represents the world's first comprehensive, binding legislative framework for AI regulation.[33] AI systems used as medical devices or for clinical decision support are classified as "high-risk" under Annex III, Category 5, subject to the most stringent pre-deployment and post-market requirements.[34]

High-risk health AI systems under the AI Act must comply with: mandatory conformity assessments before deployment; risk management systems throughout the AI lifecycle; data governance requirements ensuring training data representativeness; technical documentation obligations; automatic operation logging to enable post-deployment auditability; transparency obligations towards deploying institutions; and technically built-in human oversight mechanisms.[35] Enforcement is backed by substantial penalties: violations of obligations for high-risk AI may attract fines of up to EUR 15 million or 3 per cent of global annual turnover.[36]

Critically for the Indian context, the EU AI Act requires that high-risk AI systems in healthcare be tested across diverse demographic groups and that bias mitigation measures be documented and auditable. The Act also imposes specific transparency obligations enabling patients and health professionals to understand the role and limitations of AI in their care—an operationalisation of the right to informed consent that Indian law currently lacks.

5.2 The United States: FDA's Regulatory Approach to AI-SaMD

The United States Food and Drug Administration (FDA) has developed a risk-based regulatory framework for AI-enabled Software as a Medical Device under its authority over medical devices under the Federal Food, Drug, and Cosmetic Act (FD&C Act), as supplemented by the 21st Century Cures Act, 2016.[37] The FDA's 2021 Action Plan for AI/ML-Based SaMD introduced the concept of a "Predetermined Change Control Plan" (PCCP)—a pre-approved framework permitting AI systems to adapt and update their algorithms within defined bounds without requiring full pre-market re-approval.[38]

This approach recognises that AI systems, unlike static medical devices, are adaptive—their performance changes as they encounter new data. The FDA's framework thus provides for lifecycle regulation rather than one-time pre-market approval, a design principle of significant relevance for India. The FDA's 2024 Final Guidance on Predetermined Change Control Plans for AI/ML-Enabled Device Software Functions further required sponsors to address algorithm transparency, performance testing across diverse demographic subgroups including by sex, race, age, and comorbidity status, and bias mitigation measures.[39]

6. Towards a Rights-Centric Framework for AI Governance in Indian Healthcare

Based on the foregoing constitutional analysis, identification of regulatory gaps, and comparative survey, the following framework is proposed for a comprehensive legislative and institutional response. It is anchored in five principles: constitutional compliance, transparency and explainability, non-discrimination, accountability and liability, and participatory governance.

6.1 Enact a Digital Health and Artificial Intelligence Act (DHAIA)

India requires a dedicated, standalone statute governing AI in healthcare. The DHAIA should establish a risk-tiered classification system for health AI applications, modelled on the EU AI Act but calibrated to Indian constitutional values and health equity imperatives. AI systems used for clinical diagnosis, prognosis, treatment recommendation, drug safety monitoring, insurance underwriting, and public health surveillance should be classified as high-risk and subject to mandatory pre-deployment conformity assessment, algorithmic bias audits, explainability requirements, and post-deployment performance monitoring. The DHAIA should amend the Drugs and Cosmetics Act, 1940 to insert a definition of "AI-enabled Software as a Medical Device" and create a statutory pre-market authorisation

[32] Digital Personal Data Protection Act, 2023, ss 18-28 (India) (establishing the Data Protection Board of India and its functions).

[33] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).

[34] Regulation (EU) 2024/1689, Annex III, para 5(a).

[35] Regulation (EU) 2024/1689, arts 9-17 (requirements for high-risk AI systems).

[36] Regulation (EU) 2024/1689, art 99 (penalties).

[37] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, ss 3060-3062 (2016) (U.S.) (establishing a regulatory framework for software functions as medical devices).

[38] U.S. Food and Drug Administration, "Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan" (Jan. 2021).

[39] U.S. Food and Drug Administration, "Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions" (Final Guidance, 2024).

pathway for such devices, administered by the CDSCO under enhanced technical capacity.

6.2 Statutory Explainability Mandate and Right to Reason in Healthcare AI

The DHAIA should incorporate a statutory right to explanation for AI-influenced healthcare decisions. Any individual who receives a diagnosis, prognosis, treatment recommendation, or insurance determination that was materially influenced by an AI system should be entitled to: (a) a plain-language explanation of the factors that influenced the AI's output; (b) the confidence level of the AI's assessment; and (c) the material limitations of the system. This right would operationalise the constitutional requirement of reasoned decision-making and enable meaningful informed consent consistent with *Samira Kohli.*[40]

6.3 Mandatory Algorithmic Bias Audits and Dataset Representativeness

To give substantive content to the equality guarantee under Article 14, the DHAIA should mandate that all high-risk health AI systems undergo pre-deployment algorithmic bias audits and post-deployment performance monitoring, disaggregated by gender, age, caste, socioeconomic status, geographic location (urban/rural), and disability status. AI developers and deployers should be required to demonstrate that training datasets are representative of the diverse Indian population, with particular attention to historically marginalised communities. Audit reports should be made publicly available to enable civil society scrutiny, and non-compliance should attract civil and regulatory penalties administered by the proposed Digital Health Regulatory Authority (DHRA).[41]

6.4 Statutory Liability Framework for AI-Assisted Medical Negligence

The DHAIA should introduce a statutory liability framework addressing the multi-party attribution challenge in AI-assisted clinical negligence. A tiered model is proposed: (a) primary liability for AI developers for design defects or algorithmic failures; (b) secondary liability for healthcare institutions for negligent deployment or inadequate human oversight; and (c) residual State liability for AI deployed through public health programmes. A no-fault compensation fund should be established for patients harmed by failures of government-deployed health AI systems, ensuring victims are not left without remedy by the difficulties of proving causation through opaque algorithmic chains.[42]

6.5 Establishment of an Independent Digital Health Regulatory Authority (DHRA)

The existing regulatory landscape for digital health AI is fragmented across the CDSCO, IRDAI, the National Health Authority, and the prospective Data Protection Board. The DHAIA should establish an independent Digital Health Regulatory Authority (DHRA) with the following mandate: pre-market authorisation of high-risk health AI systems; post-market surveillance and incident reporting; algorithmic audit certification; standard-setting for health data representativeness; and adjudication of patient complaints relating to AI-driven healthcare decisions. The DHRA should include domain experts in medicine, data science, law, public health, and civil society representatives from marginalised communities, ensuring participatory and technically informed governance.[43]

6.6 Reform of the DPDP Act: Health AI-Specific Protections

The DPDP Act, 2023 should be amended to: (a) restore the right to explanation for automated decisions that significantly affect health and healthcare, drawing on the provision omitted from Clause 19 of the 2019 Bill; (b) narrow the state exemption under Section 17 to preclude its application to AI systems deployed in healthcare settings; (c) require mandatory Data Protection Impact Assessments (DPIAs) prior to deployment of AI systems that process health data at scale; and (d) vest the Data Protection Board with specialised healthcare AI jurisdiction. These amendments would align India's data protection framework with the constitutional privacy standards articulated in *Puttaswamy* and with evolving international best practice.

7. Conclusion

The integration of Artificial Intelligence into India's healthcare ecosystem is an unfolding constitutional reality. As AI systems increasingly shape who receives a diagnosis, who is covered by health insurance, which drugs reach regulatory approval, and how public health resources are allocated, they directly determine the substantive content of the right to health as a constitutional entitlement. India's existing legal architecture—the Drugs and Cosmetics Act, the DPDP Act, the Telemedicine Guidelines, and the ABDM's administrative framework—is insufficient to govern this reality.

The constitutional framework, however, provides a strong normative foundation. Articles 14, 21, and 47 of the Constitution, read through the lens of *Puttaswamy*'s privacy jurisprudence and the Supreme Court's doctrine of constitutional morality, demand that AI-driven health

[40]Citron DK, Pasquale F. The scored society: due process for automated predictions. Washington Law Review. 2014;89(1):1-33.

[41]Barocas S, Selbst AD. Big Data's disparate impact. California Law Review. 2016;104(3):671-732. DOI: 10.15779/Z38BG31.

[42]Engstrom DF, et al. Government by algorithm: artificial intelligence in federal administrative agencies. Yale Law Journal. 2021;130(6):1695-1802.

[43]Yeung K. Algorithmic regulation: a critical interrogation. Regulation and Governance. 2018;12(4):505-523. DOI: 10.1111/rego.12158.

governance be transparent, non-discriminatory, procedurally fair, and subject to effective legal accountability. These are not aspirational goals but enforceable constitutional standards.

The proposed Digital Health and Artificial Intelligence Act, together with targeted amendments to the DPDP Act and the creation of an independent Digital Health Regulatory Authority, would translate these constitutional imperatives into operational legal obligations. The international experience of the EU AI Act and the FDA's lifecycle regulatory model for AI-SaMD demonstrates that robust, rights-centric AI governance and technological innovation are mutually reinforcing, not antithetical. India, with its established constitutional tradition of expansive fundamental rights jurisprudence and urgent public health imperatives, is positioned to develop a globally influential model of equitable AI health governance.

Ultimately, the legitimacy of AI in Indian healthcare must be earned through demonstrated commitment to constitutional values—not assumed from technical sophistication. The right to health, as the Supreme Court has consistently held, is inseparable from the right to life. A digital health system that is opaque, biased, unaccountable, or inaccessible to the poor and marginalised fails the constitutional test—regardless of its algorithmic efficiency. The regulation of artificial intelligence in healthcare is therefore not merely a policy necessity but a constitutional imperative.

References

1. Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37 (India).
2. Consumer Education and Research Centre v. Union of India, (1995) 3 SCC 42 (India).
3. State of Punjab v. Mohinder Singh Chawla, (1997) 2 SCC 83 (India).
4. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
5. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
6. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (India).
7. Samira Kohli v. Dr. Prabha Manchanda, (2008) 2 SCC 1 (India).
8. Jacob Mathew v. State of Punjab, (2005) 6 SCC 1 (India).
9. Ajay Hasia v. Khalid Mujib Sehravardi, (1981) 1 SCC 722 (India).
10. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
11. Medical Devices Rules, 2017, S.O. 2739(E), Ministry of Health and Family Welfare, Government of India (2017), as amended by Medical Devices (Amendment) Rules, 2020.
12. New Drugs and Clinical Trials Rules, 2019, G.S.R. 227(E), Ministry of Health and Family Welfare, Government of India (2019).
13. Medical Council of India, Telemedicine Practice Guidelines, 2020, Gazette of India Extraordinary (Mar. 25, 2020), Part III, Section 4.
14. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, Gazette of India (Apr. 11, 2002) (India).
15. Insurance Regulatory and Development Authority of India, IRDAI (Insurance Products) Regulations, 2024 (India).
16. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689).
17. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices, 2017 O.J. (L 117).
18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
19. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016) (U.S.).
20. Ministry of Health and Family Welfare, Government of India, Ayushman Bharat Digital Health Mission: Operational Guidelines. National Health Authority; 2022.
21. National Health Authority, ABDM Health Data Management Policy. Government of India; 2022.
22. Central Drugs Standard Control Organisation. Guidance Document on Artificial Intelligence and Machine Learning-Based Software as Medical Devices (Draft). New Delhi: CDSCO; 2024.
23. U.S. Food and Drug Administration. Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan. U.S. FDA; 2021.
24. U.S. Food and Drug Administration. Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions. Final Guidance. U.S. FDA; 2024.
25. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019;366(6464):447-453. DOI: 10.1126/science.aax2342.
26. Sharma T, et al. Aarogya Setu: India's COVID-19 contact tracing application—a legal and privacy analysis. Journal of Law and the Biosciences. 2021;8(1):lsab017. DOI: 10.1093/jlb/lsab017.
27. Gulshan V, et al. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. JAMA. 2016;316(22):2402-2410. DOI: 10.1001/jama.2016.17216.
28. Barocas S, Selbst AD. Big Data's disparate impact. California Law Review. 2016;104(3):671-732. DOI: 10.15779/Z38BG31.

29. Citron DK, Pasquale F. The scored society: due process for automated predictions. Washington Law Review. 2014;89(1):1-33.
30. Engstrom DF, et al. Government by algorithm: artificial intelligence in federal administrative agencies. Yale Law Journal. 2021;130(6):1695-1802.
31. Yeung K. Algorithmic regulation: a critical interrogation. Regulation and Governance. 2018;12(4):505-523. DOI: 10.1111/rego.12158.
32. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge: Harvard University Press; 2015.
33. Eubanks V. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press; 2018.
34. Grand View Research. India Artificial Intelligence in Healthcare Market Size Report 2024. 2024. Available at: https://www.grandviewresearch.com.
35. Personal Data Protection Bill, 2019No. 373-C, Lok Sabha (India) (lapsed).