REGULATING AI IN HEALTHCARE: LEGAL FRAMEWORKS AND CHALLENGES

M Kalaivani, Guest Lecturer, Government Law College, Vellore

ABSTRACT

The integration of Artificial Intelligence (AI) into healthcare systems has significantly transformed medical diagnosis, treatment planning, patient monitoring, and health data management. AI-driven technologies promise enhanced efficiency, accuracy, and accessibility in healthcare delivery; however, their rapid deployment raises complex legal, ethical, and regulatory concerns. This research paper critically examines the existing legal frameworks governing the use of AI in healthcare and analyses the challenges associated with regulating such technologies in a rights-based legal system. The AI applications intersect with core legal principles such as patient consent, data protection, medical negligence, and accountability. In the Indian context, the paper evaluates the applicability of existing laws, including healthcare regulations, information technology laws, and the Digital Personal Data Protection Act, 2023, highlighting the absence of AI-specific legislation in the medical sector. It further examines the role of regulatory authorities and policy guidelines in overseeing AI-enabled healthcare practices. A comparative perspective is adopted by analysing international regulatory approaches such as the European Union's AI Act, World Health Organization guidelines, and regulatory standards followed in the United States, to identify best practices and regulatory gaps. The addresses key challenges posed by AI in healthcare, including algorithmic bias, lack of transparency, data security risks, and the difficulty of attributing liability for AI-induced medical errors. These challenges raise serious concerns regarding patient safety, autonomy, and the protection of fundamental rights such as privacy and human dignity. Through doctrinal and comparative analysis, the development of a comprehensive legal framework that ensures accountability, transparency, and ethical deployment of AI technologies in healthcare. The effective regulation of AI in healthcare requires a balanced approach that promotes innovation while safeguarding patient rights, ensuring legal certainty, and maintaining public trust in AI-driven medical systems.

Keywords: Artificial Intelligence (AI), Healthcare Regulation, Data Protection, Medical Liability, Ethical AI.

INTRODUCTION

Artificial Intelligence (AI) has emerged as a transformative force in the healthcare sector, reshaping traditional medical practices through advanced data analytics, machine learning algorithms, and automated decision-making systems. From early disease detection and diagnostic imaging to personalised treatment plans and robotic surgeries, AI technologies are increasingly integrated into healthcare delivery across the world. These innovations promise improved accuracy, efficiency, and accessibility of medical services, particularly in resource-constrained environments. However, the growing reliance on AI in healthcare also raises profound legal and ethical questions, especially when such technologies directly influence clinical decisions affecting human life and well-being.

In India, the rapid digitalisation of healthcare, coupled with government initiatives promoting digital health ecosystems, has accelerated the adoption of AI-driven tools in both public and private healthcare institutions. AI systems are now used to analyse electronic health records, predict disease outbreaks, assist in diagnostics, and support telemedicine services. While these developments offer significant benefits, they operate within a legal framework that was largely designed for conventional medical practices and does not adequately address the unique risks posed by AI technologies. Existing healthcare and technology laws provide fragmented regulation, resulting in uncertainty regarding accountability, patient rights, and compliance standards.

One of the most pressing concerns arising from AI in healthcare is the protection of sensitive health data. AI systems rely heavily on vast amounts of personal and medical data, making issues of data privacy, informed consent, and cybersecurity central to legal discourse. The potential misuse of health data, algorithmic bias, and lack of transparency in AI decision-making processes further complicate the regulatory landscape. These challenges directly impact fundamental rights such as the right to privacy, bodily autonomy, and human dignity, necessitating careful legal scrutiny.

Another critical issue is the question of liability when AI-assisted medical decisions lead to harm. Traditional doctrines of medical negligence are premised on human judgment and professional expertise, whereas AI systems introduce multiple actors, including developers, healthcare providers, and data controllers. This diffusion of responsibility complicates the attribution of legal liability and highlights the inadequacy of existing legal doctrines to address AI-related harms effectively.

Against this backdrop, this paper seeks to analyse the legal frameworks governing AI in healthcare and examine the challenges associated with regulating such technologies. By adopting a doctrinal and comparative approach, the study aims to assess the sufficiency of current laws, identify regulatory gaps, and propose legal principles that can ensure responsible, ethical, and rights-oriented deployment of AI in healthcare systems. Ultimately, the paper underscores the need for a comprehensive and forward-looking regulatory framework that balances technological innovation with the protection of patient rights and public trust.

AI APPLICATIONS IN HEALTHCARE

Artificial Intelligence has become an integral component of modern healthcare by enabling data-driven decision-making, predictive analytics, and automation of complex medical processes. AI applications in healthcare extend across diagnosis, treatment, patient monitoring, and large-scale health data management. While these technologies enhance efficiency and accuracy, they also introduce legal concerns relating to privacy, consent, reliability, and accountability. Understanding the functional scope of AI in healthcare is essential to evaluating the adequacy of existing legal frameworks regulating its use.

Diagnostic and Predictive AI Tools

AI-based diagnostic tools are increasingly used to analyse medical images, pathology reports, genetic data, and electronic health records to detect diseases at early stages. Machine learning algorithms assist in identifying conditions such as cancer, cardiovascular diseases, and neurological disorders with a level of speed and precision that often surpasses human capacity. Predictive AI tools also assess patient data to forecast disease progression, hospital readmission risks, and potential outbreaks.

From a legal perspective, such tools rely heavily on sensitive personal health data, triggering privacy and data protection concerns. The Supreme Court in **District Registrar and Collector, Hyderabad v. Canara Bank**[1] recognised informational privacy as part of Article 21, holding that access to personal records without adequate legal safeguards violates the right to privacy.

[1] District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496

Although the case involved financial data, its reasoning extends to medical data, which is even more sensitive. In addition, the **Digital Personal Data Protection Act, 2023** categorises health data as personal data requiring lawful processing and purpose limitation, placing obligations on entities deploying diagnostic AI systems.

AI in Treatment, Surgery and Patient Monitoring

AI is now actively involved in treatment planning, robotic-assisted surgeries, and continuous patient monitoring through wearable devices and remote health platforms. AI-driven systems assist doctors in determining optimal treatment options, managing drug dosages, and performing precision surgeries. Patient monitoring technologies use AI to track vital signs in real time, enabling early intervention and reducing human error.

However, the integration of AI into treatment raises complex liability issues when errors occur. Traditional medical negligence law focuses on human conduct, whereas AI introduces automated decision-making into clinical care. In **Spring Meadows Hospital v. Harjol Ahluwalia**[2], the Supreme Court emphasised the duty of care owed by medical professionals and hospitals to patients. When AI systems influence clinical decisions, this duty becomes diffused between healthcare providers and technology developers, creating uncertainty regarding legal accountability. The absence of specific statutory standards for AI-assisted treatment highlights the need for clearer regulatory guidance to protect patient safety.

Use of Big Data, Algorithms and Machine Learning in Medicine

Big data analytics and machine learning form the backbone of AI-driven healthcare systems. These technologies aggregate massive volumes of patient data to identify patterns, improve medical research, and enhance public health planning. While such data-driven approaches contribute to medical innovation, they raise concerns about algorithmic bias, transparency, and informed consent. Algorithms trained on biased or incomplete data may result in discriminatory outcomes, disproportionately affecting vulnerable populations.

The Supreme Court's decision in **Selvi v. State of Karnataka**[3] is particularly relevant in this context. The Court held that involuntary extraction and analysis of personal data without

[2] Spring Meadows Hospital v. Harjol Ahluwalia (1998) 4 SCC 39
[3] Selvi v. State of Karnataka (2010) 7 SCC 263

consent violates personal liberty and mental privacy under Article 21[4]. Although the case addressed investigative techniques, its principles apply to medical AI systems that process patient data without meaningful consent or transparency. Furthermore, Section 6 of the **DPDP Act, 2023** mandates free, informed, and specific consent for data processing, reinforcing patient autonomy in AI-driven healthcare environments.

EXISTING LEGAL AND REGULATORY FRAMEWORKS

The regulation of Artificial Intelligence in healthcare in India presently operates through a combination of general medical laws, technology statutes, data protection legislation, and administrative guidelines rather than a unified AI-specific framework. While these laws provide partial oversight over healthcare practices, digital technologies, and data usage, they were not designed to address the unique risks posed by autonomous or semi-autonomous AI systems. Consequently, the existing regulatory landscape remains fragmented, creating legal uncertainty in areas such as accountability, data governance, and patient protection.

Indian Legal Framework: Medical Laws, IT Act, and DPDP Act, 2023

India does not yet have a dedicated statute governing AI in healthcare; instead, regulation is derived from existing medical and technology laws. Medical practice continues to be governed by statutes such as the **National Medical Commission Act, 2019**, which sets standards for professional conduct and medical ethics, but does not expressly regulate algorithmic decision-making or AI-assisted treatment. Similarly, the **Clinical Establishments (Registration and Regulation) Act, 2010** focuses on institutional standards rather than technological accountability.

From a digital regulation perspective, the **Information Technology Act, 2000**, particularly Sections 43A and 72A[5], imposes liability for negligence in handling sensitive personal data and unauthorised disclosure. However, these provisions are limited in scope and do not account for complex AI data ecosystems. The Supreme Court in **Justice K.S. Puttaswamy v. Union of India**[6] recognised the right to privacy as a fundamental right, laying the constitutional foundation for regulating AI systems that process health data. Building on this jurisprudence,

[4] Article 21 https://share.google/rIIf2y9mvlSbUBR24
[5] Information Technology Act, 2000 under Sections 43A and 72A https://share.google/V5CIoEmIWaqUE7VVq
[6] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

the **Digital Personal Data Protection Act, 2023** introduces consent-based processing, purpose limitation, and data fiduciary obligations, with health data receiving heightened protection. Nevertheless, broad exemptions granted to the State raise concerns about unchecked use of AI in public healthcare systems.

Role of Regulatory Bodies (MoHFW, ICMR, NMC)

Regulatory oversight of AI in healthcare is primarily exercised through executive and advisory bodies rather than binding legislation. The **Ministry of Health and Family Welfare (MoHFW)** plays a central role in shaping digital health policy through initiatives such as the National Digital Health Mission. The **Indian Council of Medical Research (ICMR)** has issued ethical guidelines for biomedical research and AI applications, emphasising transparency, patient consent, and accountability. While these guidelines are influential, they lack statutory enforceability.

The **National Medical Commission (NMC)** regulates medical education and professional conduct but has yet to establish comprehensive standards governing AI-assisted clinical decision-making. The importance of regulatory accountability was underscored by the Supreme Court in **Madras Bar Association v. Union of India**[7], where the Court stressed that regulatory bodies exercising significant powers must function within constitutional limits and maintain institutional independence. This principle is relevant to healthcare regulators overseeing AI technologies with direct implications for fundamental rights.

International Frameworks: WHO Guidelines, EU AI Act, and FDA Regulations

At the international level, regulatory approaches provide useful comparative insights. The **World Health Organization (WHO)** has issued guidance on ethical AI in health, focusing on safety, explainability, human oversight, and inclusiveness. The **European Union's AI Act** adopts a risk-based regulatory model, categorising AI systems used in healthcare as "high-risk" and subjecting them to strict compliance obligations, including human supervision and accountability mechanisms. In the United States, the **Food and Drug Administration (FDA)** regulates AI-based medical devices through pre-market approvals and post-deployment monitoring.

[7] Madras Bar Association v. Union of India (2021) 7 SCC 369

Indian courts have recognised the value of international best practices in rights-based regulation. In **Vishaka v. State of Rajasthan**[8], the Supreme Court held that international norms can inform domestic legal frameworks in the absence of specific legislation. Applying this principle, global AI governance standards can guide India in developing a comprehensive and rights-oriented regulatory framework for AI in healthcare.

PRIVACY, DATA PROTECTION AND PATIENT CONSENT

The deployment of Artificial Intelligence in healthcare fundamentally depends on the collection, processing, and analysis of vast quantities of personal medical data. While such data-driven systems enhance efficiency and clinical accuracy, they also raise serious concerns relating to privacy, informed consent, and data security. Given the intimate nature of health information, AI-enabled healthcare systems must operate within a robust legal framework that safeguards patient autonomy and prevents misuse, surveillance, and unauthorised data exploitation.

Health Data as Sensitive Personal Data

Health data constitutes one of the most sensitive categories of personal information, as it reveals intimate details about an individual's physical and mental condition. The Supreme Court in **Justice K.S. Puttaswamy (Aadhaar) v. Union of India**[9] categorically recognised informational privacy as an intrinsic part of Article 21 and held that medical and biometric data demand a higher degree of protection. The Court emphasised that any intrusion into such data must satisfy the tests of legality, necessity, and proportionality.

Statutorily, the **Digital Personal Data Protection Act, 2023** reinforces this constitutional protection by imposing strict obligations on data fiduciaries processing personal data, including health-related information. Purpose limitation, data minimisation, and security safeguards are central principles under the Act, which are particularly relevant when AI systems continuously process patient data for diagnostics, monitoring, and predictive analytics.

Consent, Data Sharing and Secondary Use of Medical Data

In AI-driven healthcare, patient consent often extends beyond immediate treatment to include

[8] Vishaka v. State of Rajasthan (1997) 6 SCC 241

[9] Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018) 1 SCC 1

data sharing for research, training algorithms, and secondary commercial use. This raises questions about whether consent is truly informed and specific. In **R. Rajagopal v. State of Tamil Nadu**[10], the Supreme Court recognised the right to privacy as the right to be let alone and held that personal information cannot be published or used without consent, except in limited circumstances. This principle directly applies to the secondary use of medical data by AI developers and healthcare institutions.

Further, in **Binoy Viswam v. Union of India**[11], the Court upheld conditional data collection but stressed that consent-based data usage must be proportionate and purpose-bound. Under the **DPDP Act, 2023**, consent must be free, informed, specific, and revocable, posing compliance challenges for AI systems that rely on continuous data ingestion and algorithmic learning.

Surveillance, Data Breaches and Cybersecurity Risks

AI-enabled healthcare infrastructures also create risks of covert surveillance, unauthorised access, and large-scale data breaches. Centralised health databases and interconnected AI systems may expose patients to profiling and monitoring beyond clinical necessity. The Supreme Court in **PUCL v. Union of India**[12] held that surveillance without adequate procedural safeguards violates the right to privacy, even when undertaken in the interest of public order or security. Although the case involved telephone tapping, its principles apply equally to digital health surveillance.

Additionally, cyber vulnerabilities in AI systems can lead to massive data breaches, undermining patient trust. In **Shreya Singhal v. Union of India**[13], the Court highlighted the chilling effect that unchecked State and private control over digital spaces can have on individual freedoms. This reasoning underscores the need for strong cybersecurity standards and accountability mechanisms to prevent misuse of AI-driven healthcare data.

LIABILITY AND ACCOUNTABILITY IN AI-DRIVEN HEALTHCARE

The increasing integration of Artificial Intelligence into clinical decision-making has blurred

[10] R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632
[11] Binoy Viswam v. Union of India (2017) 7 SCC 59
[12] PUCL v. Union of India (1997) 1 SCC 301
[13] Shreya Singhal v. Union of India (2015) 5 SCC 1

traditional notions of responsibility in healthcare delivery. While AI systems assist in diagnosis, treatment planning, and patient monitoring, they do not operate in isolation and are embedded within human-controlled medical environments. This raises complex questions regarding liability when harm occurs, particularly concerning medical negligence, allocation of responsibility among stakeholders, and accountability for algorithmic or technological failures.

Medical Negligence and AI-Assisted Decisions

Medical negligence in India is traditionally assessed based on the standard of reasonable care expected from a competent medical professional. In **Jacob Mathew v. State of Punjab**[14], the Supreme Court held that negligence arises when a doctor fails to exercise the level of skill and care that a reasonably competent practitioner would have exercised under similar circumstances. In AI-assisted healthcare, this principle implies that reliance on AI tools does not absolve doctors of their professional duty. Physicians must apply independent clinical judgment and cannot blindly follow algorithmic outputs without scrutiny.

Similarly, in **Kusum Sharma v. Batra Hospital**[15], the Court emphasised that courts should distinguish between acceptable medical risks and actionable negligence. If an AI recommendation is used as an assistive tool and the doctor exercises due diligence, liability may not arise. However, unquestioned reliance on flawed AI outputs may amount to negligence if it deviates from accepted medical standards.

Liability of Doctors, Hospitals and AI Developers

The question of who bears liability becomes more complex when harm results from AI-driven decisions. In **Spring Meadows Hospital v. Harjol Ahluwalia**[16], the Supreme Court held hospitals vicariously liable for negligence of medical professionals under their employment. Applying this principle, hospitals deploying AI systems may be held accountable for inadequate training, improper integration, or failure to monitor AI-assisted treatment.

Doctors remain primarily responsible for patient care, but AI developers and technology providers may also bear liability where harm arises due to defective software or misleading algorithmic design. The **Consumer Protection Act, 2019** expands the scope of liability by

[14] Jacob Mathew v. State of Punjab (2005) 6 SCC 1
[15] Kusum Sharma v. Batra Hospital (2010) 3 SCC 480
[16] Spring Meadows Hospital v. Harjol Ahluwalia (1998) 4 SCC 39

recognising “product liability,” allowing claims against manufacturers and service providers for harm caused by defective products or deficient services. AI-based medical tools, when supplied commercially, may fall within this framework.

Product Liability and Algorithmic Errors

Algorithmic errors, data bias, and faulty training models pose serious risks in AI-enabled healthcare. Under **Section 84 of the Consumer Protection Act, 2019**[17], a product manufacturer is liable if a defect in design, manufacturing, or instructions causes harm. If an AI diagnostic system produces erroneous outputs due to flawed algorithms or inadequate validation, developers and suppliers may be held liable for resultant injury.

Indian courts have increasingly recognised technological accountability in healthcare contexts. In **Dr. Balram Prasad v. Dr. Kunal Saha**[18], the Supreme Court awarded compensation for gross medical negligence, underscoring that advanced technology cannot justify substandard care. This reasoning supports the view that AI systems must meet high safety and reliability standards, and failures must attract legal consequences to ensure patient protection and ethical innovation.

ETHICAL AND CONSTITUTIONAL CHALLENGES

The deployment of Artificial Intelligence in healthcare raises profound ethical and constitutional concerns, as algorithmic decision-making increasingly influences matters directly affecting human life, bodily integrity, and dignity. While AI promises efficiency and accuracy, its opaque functioning, potential for bias, and limited explainability pose serious challenges to constitutional values such as equality, autonomy, and the protection of fundamental rights. These concerns necessitate a careful examination of how AI systems align with ethical principles and constitutional safeguards in India.

Bias, Discrimination and Algorithmic Transparency

AI systems are trained on large datasets that may reflect existing social and structural biases, leading to discriminatory outcomes in healthcare access, diagnosis, or treatment. Such bias can disproportionately affect marginalised communities, violating the principle of equality under

[17] Section 84 of the Consumer Protection Act, 2019 https://share.google/bOmGV4Au7P4HIfrXJ

[18] Dr. Balram Prasad v. Dr. Kunal Saha (2014) 1 SCC 384

Article 14 of the Constitution of India[19]. In **State of West Bengal v. Anwar Ali Sarkar**[20], the Supreme Court held that arbitrary state action lacking rational classification violates Article 14. Applying this reasoning, opaque AI systems producing unequal outcomes without transparency or justification may be constitutionally suspect.

Further, the lack of algorithmic transparency undermines accountability and trust. In **Kranti Associates v. Masood Ahmed Khan**[21], the Court emphasised that reasoned decision-making is an essential component of fairness and the rule of law. AI systems that function as "black boxes" challenge this principle, as affected patients may be unable to understand or contest medical decisions influenced by algorithms.

Right to Health, Right to Privacy and Human Dignity

The right to health has been judicially recognised as an integral part of the right to life under **Article 21**. In **Paschim Banga Khet Mazdoor Samity v. State of West Bengal**[22], the Supreme Court held that failure to provide timely medical treatment violates Article 21. AI-driven healthcare, if improperly regulated or deployed, may compromise quality of care and undermine this constitutional guarantee.

Moreover, the use of AI involves extensive processing of sensitive health data, directly implicating the right to privacy. In **District Registrar and Collector v. Canara Bank**[23], the Court recognised informational privacy as part of personal liberty. The misuse or unauthorised sharing of health data through AI systems threatens human dignity, a core constitutional value repeatedly affirmed by Indian courts.

Autonomy, Informed Consent and Explainable AI

Patient autonomy and informed consent are foundational ethical principles in medical jurisprudence. In **Samira Kohli v. Dr. Prabha Manchanda**[24], the Supreme Court held that medical procedures without informed consent violate patient autonomy and bodily integrity. In the context of AI-assisted healthcare, meaningful consent requires that patients are informed

[19] Article 14 of the Constitution of India https://share.google/rIIf2y9mvlSbUBR24
[20] State of West Bengal v. Anwar Ali Sarkar (1952 SCR 284)
[21] Kranti Associates v. Masood Ahmed Khan (2010) 9 SCC 496
[22] Paschim Banga Khet Mazdoor Samity v. State of West Bengal (1996) 4 SCC 37
[23] District Registrar and Collector v. Canara Bank (2005) 1 SCC 496
[24] Samira Kohli v. Dr. Prabha Manchanda (2008) 2 SCC 1

not only about the treatment but also about the role of AI in decision-making.

The concept of **Explainable AI (XAI)** becomes crucial in this regard. If AI-generated recommendations cannot be explained in understandable terms, patients are effectively denied informed consent. This undermines constitutional protections under Article 21 and raises ethical concerns about substituting human judgment with opaque technological processes in matters involving life and health.

CHALLENGES AND THE WAY FORWARD

Despite the growing use of Artificial Intelligence in healthcare, India lacks a comprehensive and coherent regulatory framework tailored to the unique risks posed by AI-driven medical systems. The existing legal regime is fragmented across health, technology, and data protection laws, resulting in regulatory uncertainty, weak enforcement, and inadequate safeguards for patient rights. Addressing these challenges requires targeted legislative reforms and a rights-based governance model that balances innovation with constitutional values.

Regulatory Gaps and Enforcement Challenges

One of the foremost challenges is the absence of clear legal standards governing the development, deployment, and accountability of AI systems in healthcare. While sectoral laws exist, they do not address algorithmic accountability, bias, or explainability. In **Common Cause v. Union of India**[25], the Supreme Court underscored the importance of regulatory clarity and procedural safeguards in matters affecting life and personal liberty under Article 21. Applying this reasoning, the lack of structured oversight over AI-assisted medical decisions may amount to a failure of constitutional governance.

Enforcement mechanisms also remain weak due to overlapping institutional jurisdictions. Regulatory bodies often lack technical expertise to audit AI systems effectively, leading to regulatory capture or under-enforcement. This regulatory vacuum risks unchecked technological expansion without adequate patient protection.

Need for AI-Specific Healthcare Legislation

India's current legal framework does not sufficiently address the unique characteristics of AI,

[25] Common Cause v. Union of India (2018) 5 SCC 1

such as autonomous learning, probabilistic decision-making, and cross-border data flows. In **Vineet Narain v. Union of India**[26], the Supreme Court held that institutional accountability and independent oversight are essential for governance involving complex systems. This principle supports the need for dedicated AI legislation with clear standards for risk assessment, certification, and continuous monitoring in healthcare settings.

An AI-specific healthcare law should clearly define the roles and responsibilities of doctors, hospitals, and AI developers, establish liability thresholds, and mandate transparency obligations. Such legislation would also align domestic law with emerging global best practices, ensuring legal certainty and public trust.

Recommendations for Rights-Based and Ethical AI Governance

A rights-based approach to AI governance must place constitutional values at its core. In **Justice K.S. Puttaswamy v. Union of India**[27], the Supreme Court emphasised that technological progress cannot override fundamental rights. Accordingly, AI systems in healthcare should comply with principles of legality, necessity, and proportionality.

Mandatory impact assessments, algorithmic audits, and explainability requirements should be introduced to prevent discrimination and arbitrariness. Additionally, informed consent frameworks must be strengthened to ensure patient autonomy. Establishing an independent AI regulatory authority with multidisciplinary expertise would further enhance oversight and accountability. Ultimately, ethical and constitutional governance of AI in healthcare is essential to ensure that innovation serves human welfare rather than undermining dignity, equality, and trust in medical institutions.

CONCLUSION

Artificial Intelligence is rapidly transforming healthcare in India, offering unprecedented opportunities for enhancing diagnostics, treatment, patient monitoring, and medical research. Its integration promises greater efficiency, precision, and accessibility, particularly in resource-limited settings. However, the deployment of AI in healthcare is accompanied by significant legal, ethical, and constitutional challenges that cannot be overlooked. The collection, storage,

[26] Vineet Narain v. Union of India (1998) 1 SCC 226
[27] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

and processing of sensitive health data, the opacity of algorithmic decision-making, and the diffusion of accountability among healthcare providers, hospitals, and AI developers raise complex issues that existing legal frameworks only partially address.

Indian constitutional jurisprudence, particularly the Supreme Court's recognition of the right to privacy in **Justice K.S. Puttaswamy v. Union of India**, provides a foundational safeguard for personal data and patient autonomy. Coupled with statutory instruments such as the **Digital Personal Data Protection Act, 2023**, and traditional healthcare laws like the **National Medical Commission Act, 2019**, there exists a preliminary regulatory base for overseeing AI applications. Nevertheless, these measures are fragmented, reactive, and lack specificity for AI-enabled medical systems. Current regulations fail to comprehensively address algorithmic bias, explainability, informed consent, cybersecurity risks, and liability for AI-induced harm, leaving patients vulnerable and healthcare providers uncertain about legal accountability.

International experiences, such as the **EU AI Act**, **FDA regulations in the United States**, and **WHO ethical guidelines**, highlight the importance of risk-based governance, transparency, and mandatory human oversight in high-stakes AI applications. Comparative perspectives underline the necessity for India to adopt a proactive, context-specific, and rights-oriented regulatory framework that balances innovation with patient protection, constitutional rights, and ethical standards.

A forward-looking regulatory approach should prioritise clear standards for AI system validation, mandatory algorithmic audits, explainability requirements, and robust liability mechanisms. Institutional oversight by empowered regulatory authorities, coupled with enforceable ethical guidelines, can ensure that AI-driven healthcare respects autonomy, equality, and human dignity. Moreover, continuous public engagement and awareness initiatives are crucial to build trust and social legitimacy for AI technologies in healthcare.

AI holds transformative potential for improving healthcare delivery in India, its benefits can only be realised if legal and ethical safeguards are strengthened. Developing a comprehensive AI-specific healthcare framework that integrates constitutional safeguards, statutory regulations, ethical norms, and technical standards is imperative. Such a framework will ensure that AI serves as a tool to enhance human welfare, protect patient rights, and foster equitable, transparent, and accountable healthcare systems.

REFERENCES

Books

1. R. Goel, *Artificial Intelligence in Healthcare: Legal, Ethical and Policy Perspectives*, New Delhi: LexisNexis, 2022.

2. S. Vashisht, *Health Law in India: Regulatory and Policy Issues*, New Delhi: Eastern Book Company, 2021.

3. P. Sharma, *Data Protection and Privacy in India*, 2nd Edition, New Delhi: Universal Law Publishing, 2020.

4. K. Choudhary, *AI and Healthcare: Ethics, Liability, and Governance*, Oxford University Press, 2022.

5. A. Bhatia, *Emerging Legal Issues in AI and Digital Health*, Springer, 2021.

6. N. Agarwal, *Law, Ethics and Artificial Intelligence in Medicine*, Cambridge University Press, 2022.

Statutes and Legal Provisions

1. The Constitution of India, 1950.

2. National Medical Commission Act, 2019.

3. Clinical Establishments (Registration and Regulation) Act, 2010.

4. Information Technology Act, 2000 -Sections 43A, 72A.

5. Digital Personal Data Protection Act, 2023 - Section 6: Consent for sensitive data.

6. Consumer Protection Act, 2019 - Section 84: Product liability.

Journal Articles

1. Singh, A., "Legal and Ethical Challenges of AI in Healthcare," *Indian Journal of*

Medical Ethics, Vol. 18, Issue 3, 2021, pp. 45-56.

2. Gupta, R., “AI and Liability in Indian Healthcare Law,” *National Law School Review*, 2020, pp. 112-130.

3. Rao, S., “Privacy Implications of Digital Health Data in India,” *Journal of Law and Technology*, Vol. 12, 2022, pp. 78-95.

4. Kapoor, N., “Algorithmic Bias and Patient Safety: Legal Perspectives,” *Indian Journal of Legal Studies*, 2021, pp. 23-41.

5. Ramesh, P., “AI, Ethics, and Data Protection in Indian Hospitals,” *International Journal of Law and Technology*, 2021, pp. 101–125.

Web Resources / Reports

1. Ministry of Health and Family Welfare (MoHFW), *National Digital Health Mission Guidelines*, Government of India, 2020. Available at: https://www.ndhm.gov.in

2. World Health Organization (WHO), *Ethics and Governance of Artificial Intelligence for Health*, 2021. Available at: https://www.who.int/publications/i/item/9789240030004

3. European Commission, *Proposal for a Regulation on Artificial Intelligence (AI Act)*, 2021. Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

4. U.S. Food and Drug Administration (FDA), *Artificial Intelligence and Machine Learning in Software as a Medical Device*, 2021. Available at: https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning.