

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ARTIFICIAL INTELLIGENCE IN HEALTHCARE: AN INDIAN PERSPECTIVE

AUTHORED BY - EVANIA IRENE K

2nd Year LLM (Cyber Law)

The Tamil Nadu Dr. Ambedkar Law University, Chennai

Abstract

Artificial Intelligence (AI) is increasingly becoming an integral part of modern healthcare, assisting doctors in diagnosing diseases, analysing medical images, monitoring patients, predicting health risks, developing medicines, and managing healthcare services, thereby improving the speed, accessibility, and efficiency of healthcare delivery. However, the growing reliance on AI also raises a critical legal question regarding responsibility when an AI system makes or contributes to an incorrect medical decision, particularly in India where the adoption of AI in healthcare is expanding rapidly but a comprehensive legal framework specifically governing medical AI has yet to emerge. This paper examines the major legal, ethical, and regulatory challenges associated with the use of AI in the Indian healthcare sector, focusing on issues such as the privacy and security of patients' health data, informed consent, the use of personal data for training AI systems, algorithmic bias, the lack of transparency in AI-generated recommendations, medical errors, and the allocation of liability among developers, healthcare professionals, and healthcare institutions. It further analyses the role and responsibilities of medical practitioners when AI is integrated into diagnosis or treatment and highlights the concern that patients may not always be aware of AI's involvement in clinical decision-making or understand how their personal data is processed. The paper argues that AI should function as a decision-support tool rather than replace human judgment and responsibility, and contends that India requires a robust governance framework that clearly allocates accountability across the lifecycle of AI systems while ensuring strong protection of health data, meaningful human oversight, regular testing and monitoring of AI systems, measures to identify and mitigate algorithmic bias, effective cybersecurity safeguards, and accessible legal remedies for patients who suffer harm. It concludes that the responsible governance of AI in healthcare must strike a balance between fostering technological innovation and safeguarding patient safety, privacy, accountability, and public trust.

Keywords: Artificial Intelligence, Healthcare, Cybersecurity, Privacy, AI Governance.

1. Introduction

Artificial Intelligence (AI) is quickly changing the landscape of healthcare by improving disease diagnosis, medical imaging, clinical decision-making, drug development, patient monitoring, and healthcare administration. AI-driven technologies have the capability to enhance the efficiency, accessibility, and quality of healthcare services, especially in nations like India, where issues such as a lack of healthcare professionals, unequal access to medical resources, and a growing disease burden continue to challenge the healthcare system. Acknowledging this potential, the World Health Organisation (WHO) has recognised AI as a crucial instrument for strengthening healthcare systems, while stressing the importance of ethical governance, transparency, accountability, and safeguarding human rights in its application.

The integration of Artificial Intelligence (AI) into India's healthcare sector has accelerated through initiatives such as the Ayushman Bharat Digital Mission (ABDM), the digitisation of health records, and government efforts to promote AI-driven innovation. AI is increasingly used to assist in disease diagnosis, medical imaging, clinical decision-making, and healthcare administration. While these advancements improve the quality and efficiency of healthcare, they also create significant legal and ethical challenges.

A key concern is determining accountability when AI-assisted medical decisions result in patient harm. AI also raises issues relating to patient privacy, informed consent, data security, algorithmic bias, transparency, and cybersecurity. Although India has introduced the Digital Personal Data Protection Act, 2023¹ and various AI policy initiatives, it still lacks a dedicated legal framework governing AI in healthcare.

This paper examines the legal, ethical, and regulatory challenges associated with AI in India's healthcare sector, evaluates the existing legal framework, and identifies key regulatory gaps. It argues that AI should function as a decision-support tool supported by a comprehensive governance framework that ensures patient safety, protects health data, promotes transparency, allocates accountability, and maintains meaningful human oversight.

2. Understanding Artificial Intelligence in Healthcare

Artificial Intelligence (AI) refers to the ability of computer systems to perform tasks that normally require human intelligence, such as learning, reasoning, problem-solving, recognising patterns, understanding language, and making decisions. The Organisation for Economic Co-

¹ Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

operation and Development (OECD) defines AI as a machine-based system capable of generating predictions, recommendations, or decisions for human-defined objectives, while the World Health Organisation (WHO) recognises AI as a collection of technologies that enhance healthcare through intelligent data analysis, automation, and clinical decision support. AI is intended to assist healthcare professionals rather than replace them by improving the speed, accuracy, and efficiency of medical decision-making.

AI is typically divided into two categories based on its capabilities: general AI and narrow AI. Narrow AI, sometimes referred to as weak AI, is the type of AI that is now employed in healthcare, including clinical decision support, medical imaging analysis, predictive analytics, and disease detection. It carries out particular tasks within a restricted area. On the other hand, general artificial intelligence (AI) refers to a hypothetical system that is still in the development stage and is capable of carrying out any intellectual work that a human can.

The functioning of healthcare AI is primarily driven by Machine Learning (ML), a branch of AI that enables computers to learn from data and improve predictions without explicit programming. Deep Learning, a more sophisticated version, analyses complicated datasets like pathology slides and medical photographs using artificial neural networks, allowing for extremely precise illness detection. However, deep learning models are frequently criticised for what is known as the "black box" problem their inability to be explained. Generative AI is another innovative technology that can produce new text, photos, and clinical documentation. Although its use in healthcare poses questions about accuracy, privacy, and regulatory control, it also improves clinical record keeping, medication development, patient communication, and medical research².

2.2 Applications of AI in Healthcare

Artificial intelligence is now being used in almost every facet of healthcare delivery. AI technologies promote evidence-based clinical decision-making, increase operational efficiency, and improve diagnostic accuracy for healthcare providers.

Medical Imaging: AI helps radiologists diagnose abnormalities like tumours, fractures, and other disorders by analysing CT, MRI, X-ray, mammography, and ultrasound images more quickly and accurately.

Disease Diagnosis: In order to assist in the early detection of conditions including cancer, diabetes, cardiovascular disease, and neurological problems, artificial intelligence (AI)

² Sergei Polevnikov, *Advancing AI in healthcare: A comprehensive review of best practices*, ELSEVIER, 1, 2, (2023)

assesses symptoms, lab reports, medical histories, and imaging data.

Clinical Decision Support: AI-powered Clinical Decision Support Systems (CDSS) provide evidence-based recommendations on diagnosis, treatment options, and medication management, while the final clinical decision remains with the treating physician.

Predictive Analysis: In order to enable early intervention and preventative healthcare, artificial intelligence (AI) evaluates patient data to forecast illness risks, hospital readmissions, disease progression, and medical emergencies.³

Drug Discovery: By analysing biomedical data, finding possible medication candidates, and forecasting their safety and efficacy, artificial intelligence (AI) speeds up the creation of new drugs while cutting down on research expenses and time.

Personalised Medicine: AI uses genetic information, medical history, and clinical data to recommend customised treatment plans tailored to individual patient needs.

Robotic Surgery: Robotic systems with AI assistance improve control during minimally invasive operations, increase surgical precision, lower complications, and promote quicker patient recovery. **Virtual Health Assistants:** AI-powered chatbots and virtual assistants improve healthcare accessibility and engagement by offering symptom assessment, prescription reminders, appointment booking, and patient support⁴.

Hospital Administration: AI streamlines administrative functions such as appointment scheduling, billing, resource allocation, inventory management, and electronic health record management, improving operational efficiency.

Telemedicine: AI enhances telemedicine through remote consultations, patient monitoring, symptom analysis, and clinical decision support, improving access to healthcare, particularly in rural and underserved areas.

2.3 Benefits of AI in Healthcare

Artificial intelligence has the potential to greatly improve healthcare by raising the standard, effectiveness, affordability, and accessibility of medical treatments. AI serves as a decision-support technology that facilitates quicker analysis of complicated medical data, supports clinical decision making, and simplifies healthcare operations rather than taking the place of medical experts. AI has a number of advantages that improve patient outcomes and streamline

³ Eric J. Topol, High-Performance Medicine: The Convergence of Human and Artificial Intelligence, 25 Nature Med. 44 (2019).

⁴ Mohammed Yousef Shaheen, *Applications of Artificial Intelligence (AI) in healthcare: A review*, SO, 1, 3-4, (2021)

healthcare delivery as healthcare organisations use digital technologies more and more⁵.

- **Improved Diagnostic Accuracy:** AI reduces diagnostic errors by analyzing patient data, lab results, and medical images to more quickly and accurately identify diseases like diabetic retinopathy, cancer, and cardiovascular issues.
- **Early Disease Detection and Prevention:** Predictive analytics driven by AI can identify those who are at risk for chronic illnesses, allowing for preventive care, early intervention, and ongoing monitoring.
- **Personalised Treatment:** AI analyses genetic information, medical history, and treatment responses to recommend customised treatment plans tailored to individual patients.
- **Enhanced Efficiency in Healthcare Delivery:** AI allows healthcare workers to concentrate more on patient care by automating administrative duties like arranging appointments, billing, paperwork, and managing electronic health records.
- **Faster Drug Discovery and Medical Research:** By analysing biomedical data, finding possible drug candidates, and cutting down on the time and expense of conventional research, artificial intelligence (AI) speeds up the creation of new drugs.
- **Improved Access to Healthcare:** Access to healthcare is enhanced by AI-powered telemedicine, virtual health assistants, and remote patient monitoring, especially in underprivileged and rural areas.
- **Better Clinical Decision Making:** AI-powered Clinical Decision Support Systems (CDSS) offer evidence-based diagnosis and treatment suggestions, but the treating physician retains the final say⁶.
- **Public Service Surveillance:** AI supports the monitoring of disease outbreaks, analysis of epidemiological data, and prediction of infectious disease spread, enabling timely public health interventions.

Overall, AI has the potential to transform healthcare by improving patient outcomes, enhancing operational efficiency, and expanding access to quality healthcare. However, these benefits can only be fully realised through a robust legal and regulatory framework that ensures patient safety, privacy, accountability, and public trust.

⁵ A. Esteva et al., A Guide to Deep Learning in Healthcare, 25 Nature Med. 24 (2019).

⁶ The Lancet Digital Health, Artificial Intelligence in Healthcare: Within Touching Distance, 1 Lancet Digital Health e253 (2019).

3. Existing Legal Framework Governing AI in Healthcare in India

India does not presently have a dedicated statute regulating the use of Artificial Intelligence (AI) in healthcare. Rather, the Government of India's policy frameworks, data protection laws, information technology legislation, medical ethics standards, and constitutional principles all contribute to the governance of AI. These laws offer the legal framework for resolving concerns about patient safety, privacy, data protection, accountability, and professional duty even though they were not created expressly to regulate AI. The main legal and constitutional provisions pertaining to AI in healthcare are examined in the parts that follow.

3.1 Constitutional Perspective

The Constitution of India serves as the cornerstone for protecting fundamental rights that are directly affected by the use of AI in healthcare. While the Constitution does not specifically refer to AI, judicial interpretation of Article 21⁷ has expanded its scope to include the rights to health, privacy, dignity, and personal autonomy. These constitutional protections provide the framework for assessing the legality of AI-driven healthcare technologies.

3.1.1 Article 21

According to Article 21 of the Constitution, "No person shall be deprived of his life or personal liberty except according to procedure established by law." The Supreme Court has broadened the definition of the right to life through judicial interpretation to encompass the freedom to live with dignity, obtain healthcare, and make independent health-related decisions.

Article 21 is especially important in the context of AI since AI systems have a growing impact on patient care, treatment recommendations, and medical diagnosis. AI technology must function in a way that safeguards patient safety, dignity, and justice because such decisions have a direct impact on a person's life and well-being. Therefore, the fundamental foundation for mandating strong legal protections and responsibility in the application of AI in healthcare is provided by Article 21.

3.1.2 Right to Health

The Supreme Court has often ruled that the Right to Health is an essential component of Article 21, even though the Constitution does not specifically recognise it as a Fundamental Right. The Court upheld that access to healthcare is crucial to the right to life in decisions like *Consumer Education and Research Center v. Union of India* (1995) and *Paschim Banga Khet Mazdoor Samity v. State of West Bengal* (1996).

⁷ INDIA CONST. art. 21.

By boosting patient monitoring, telemedicine, disease detection, and clinical decision-making, artificial intelligence (AI) has the potential to reinforce this constitutional right. But only if AI systems are precise, trustworthy, and devoid of prejudice will these advantages be realised. Thus, it is the State's duty to guaranty that AI technologies improve rather than undermine.

3.1.3 Right to Privacy

Privacy is a major constitutional problem since the growing use of AI in healthcare necessitates the processing of massive amounts of personal health data, including medical records, diagnostic results, genetic information, and electronic health records.

An individual's control over the gathering, use, and disclosure of personal data is safeguarded by the right to privacy. Patient data must be processed legally and securely in the healthcare industry. Protecting informational privacy is crucial to preserving patient liberty and upholding public confidence because AI systems heavily rely on health data.

3.1.4 Justice K.S Puttaswamy vs. Union of India

The Supreme Court acknowledged the right to privacy as a basic right under Article 21 in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)⁸ and concluded that it encompasses informational privacy, which grants people control over their personal data, including medical information.

Given that AI systems heavily rely on patient data, the ruling is extremely pertinent to AI in healthcare. It provides the constitutional basis for regulating AI in areas like patient privacy, informed consent, and data governance by establishing that any interference with privacy must meet the requirements of legality, legitimate purpose, and proportionality.

3.2 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first comprehensive legislation governing the processing of digital personal data. Although it does not specifically regulate Artificial Intelligence (AI), it provides an important legal framework for AI-enabled healthcare, where patient data is essential for the functioning of AI systems. The Act seeks to balance the protection of personal data with the need for lawful data processing.

The Act defines personal data as any data relating to an identifiable individual, including electronic health records, medical reports, diagnostic images, prescriptions, and other patient information. While health data is not classified as a separate category of sensitive personal data, healthcare institutions are expected to implement robust security measures due to its

⁸ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.

confidential nature.

The DPDP Act is based on the principles of consent, notice, and purpose limitation. Personal data must be processed only with free, informed, and specific consent, and cannot be used beyond the stated purpose unless authorised by law or fresh consent is obtained. Hospitals, diagnostic centres, telemedicine platforms, and AI service providers function as Data Fiduciaries, responsible for lawful processing, maintaining security safeguards, and preventing data breaches. Patients, as Data Principals, have rights including access to, correction and erasure of personal data, grievance redressal, and nomination of another person to exercise these rights. The Act also permits cross-border transfer of personal data to countries not restricted by the Central Government.

The DPDP Act does not directly address AI related issues like algorithmic transparency, explainability, or accountability for AI assisted medical choices, although strengthening patient data privacy and establishing significant requirements for healthcare facilities. As such, it is not a complete legal framework for regulating AI in healthcare, but it does serve as a crucial foundation for AI governance.

3.3 Information Technology Act, 2000

Before the enactment of the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000 (IT Act)⁹ was the primary legislation governing electronic records, cybersecurity, and data protection in India. Although it does not specifically regulate Artificial Intelligence (AI), it continues to provide an important legal framework for digital healthcare.

Section 43A¹⁰ requires hospitals, healthcare institutions, and other body corporates handling electronic health information to implement reasonable security practices and may impose liability for failure to protect such data. The Act also regulates digital health platforms, telemedicine services, and cloud service providers by requiring secure handling of patient information and compliance with cybersecurity obligations¹¹.

However, the IT Act does not address AI-specific issues such as algorithmic transparency, explainability, or liability for AI-assisted medical decisions.

⁹ Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

¹⁰ Information Technology Act, No. 21 of 2000, § 43A, INDIA CODE (2000).

¹¹ Arghya Sengupta & Sushant Singh, The Information Technology Act, 2000: A Critical Analysis, 4 Indian J. L. & Tech. 1 (2008).

3.4 Ayushman Bharat Digital Mission (ABDM)

An integrated digital health ecosystem that facilitates safe, effective, and interoperable healthcare delivery throughout India is the goal of the Ayushman Bharat Digital Mission (ABDM)¹². It ensures patient privacy and consent while advancing the digitisation of healthcare.

The Ayushman Bharat Health Account (ABHA), which enables people to safely access and share their medical records, is a crucial component of ABDM. In order to enable the smooth and consent-based sharing of patient data, the mission also promotes Electronic Health Records (EHRs).

From an AI standpoint, by enhancing the accessibility and caliber of health data, ABDM offers the digital infrastructure required for AI-enabled healthcare. But the growing use of digital health records also emphasises the necessity of robust cybersecurity, accountability, transparency, and privacy policies.

3.5 National Digital Health Blueprint

The policy framework for India's digital health ecosystem is provided by the National Digital Health Blueprint (NDHB). Through electronic health records, health registries, consent management, data security, and standardised digital infrastructure, it fosters an interoperable, patient centered healthcare system.

Because it facilitates the availability of high-quality health data needed for clinical decision support, predictive analytics, and medical research, the Blueprint is important for AI in healthcare. Additionally, it places a strong emphasis on interoperability, security, informed consent, and privacy. However, because it is a policy statement, its suggestions are not legally enforceable and must be supported by legislation in order to be implemented.

3.6 NITI Aayog Documents

A number of policy publications supporting the responsible development and governance of AI in India have been released by NITI Aayog. Healthcare is a priority industry where AI can enhance diagnosis, disease prediction, and access to healthcare, according to the National Strategy for Artificial Intelligence (#AIForAll)¹³.

In addition to promoting innovation and reducing prejudice, the Responsible AI approach supports values including accountability, transparency, privacy, safety, fairness, and human

¹² AYUSHMAN BHARAT DIGITAL MISSION, <https://abdm.gov.in/>, (last visited Sep. 01, 2026)

¹³ NITI Aayog, National Strategy for Artificial Intelligence #AIForAll (2018).

oversight. However, compliance is mostly voluntary because these publications are advisory in nature and lack formal authority.

3.7 ICMR Ethical Guidelines for Applications of AI in Healthcare

To encourage the appropriate use of AI in healthcare, the Indian Council of Medical Research (ICMR)¹⁴ published the Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare in 2023. The Guidelines are founded on the following concepts and apply to researchers, healthcare practitioners, institutions, AI developers, and policymakers:

- Transparency: AI systems ought to be comprehensible and explicable.
- Accountability: AI-assisted judgments should continue to be the responsibility of developers and medical experts.
- Inclusivity: To reduce bias, representative datasets should be used when developing AI.
- Privacy: Patient information needs to be secure and treated discreetly.
- Safety: AI systems need to be regularly tested, validated, and observed.

These Guidelines are advisory in nature and not legally binding, but offering a crucial ethical basis.

3.8 Medical Regulations

The National Medical Commission (NMC) and the Registered Medical Practitioner (Professional Conduct) Regulations require doctors to exercise independent clinical judgment, obtain informed consent, maintain patient confidentiality, and adhere to professional standards of medical practice. The use of AI does not reduce the professional responsibility of healthcare practitioners, as AI should function only as a decision-support tool, with the treating physician retaining ultimate responsibility for diagnosis and treatment.

However, the existing regulations do not specifically address AI-assisted decision-making, algorithmic errors, or shared liability between doctors and AI developers, highlighting the need for a comprehensive legal framework governing AI in healthcare.

4. Legal Challenges

Artificial Intelligence (AI) has greatly enhanced medical diagnosis, treatment planning, and healthcare administration. But it has also given rise to complicated legal problems that current

¹⁴ INDIAN COUNCIL OF MEDICAL RESEARCH, <https://www.icmr.gov.in/>, (last visited Sep 02, 2026)

legislation is ill-equipped to handle. Concerns about medical negligence, responsibility allocation, patient consent, transparency, intellectual property, and cybersecurity are brought up by the growing dependence on AI. To guaranty that AI is used responsibly while upholding patient rights and preserving public confidence, these issues must be resolved.

Medical Negligence and AI: When a wrong medical judgment results in harm, it might be challenging to define who is responsible the doctor, the hospital, or the AI system which challenges the traditional concept of medical negligence. Healthcare workers must use their own clinical judgment and continue to be in charge of patient care even with AI's help.

Allocation of Liability: Determining who is responsible for medical errors caused by AI is still a significant legal concern. Doctors, hospitals, AI developers, and manufacturers may also be held accountable, but Indian law does not yet offer a precise structure for assigning blame.

AI Errors: AI systems may produce incorrect diagnoses, biased recommendations, or software errors due to poor-quality data, algorithmic bias, or technical defects. Continuous testing and monitoring are essential to minimise these risks.

Informed Consent: When AI is utilised for diagnosis or treatment, as well as when AI systems use personal health data, patients should be informed. This upholds patient autonomy and guaranties genuine informed consent.

Explainability: Many AI systems operate as "black boxes," making it challenging to comprehend the decision-making process. Explainable AI encourages responsibility, openness, and confidence in AI-assisted medical treatment¹⁵.

Intellectual Property Issues: AI raises concerns about who owns training datasets, algorithms, and medical outcomes produced by AI. To safeguard innovation and guaranty access to healthcare innovations, a well-balanced legal framework is required.

Cybersecurity Issues: Risks to AI-enabled healthcare systems include data breaches, hacks, and unauthorised access to patient data. Thus, robust cybersecurity measures are necessary to safeguard healthcare infrastructure and patient data.

5. Ethical Challenges

While Artificial Intelligence (AI) offers significant opportunities to improve healthcare delivery, its integration also raises several ethical concerns. The use of AI in diagnosis, treatment, and patient management must respect fundamental ethical principles that safeguard

¹⁵ Deepti Saraswat, *Explainable AI for Healthcare 5.0: Opportunities and Challenges*,10, IEEE ACCESS, 84486, 84493, (2022)

patient rights, dignity, and public trust. Addressing these ethical challenges is essential to ensure that AI complements human decision-making rather than undermining it¹⁶.

Patient Autonomy: Patient autonomy gives individuals the right to make informed healthcare decisions. The use of AI should support, not replace, patient participation, and patients should be informed when AI influences diagnosis or treatment.

Privacy: AI systems depend on massive amounts of personal health data, which raises questions about misuse and illegal access. Patient data must be gathered, processed, and kept safely while maintaining informational privacy in order for AI to be ethical.

Confidentiality: Sharing patient data with digital platforms and third-party providers is a common aspect of using AI. Healthcare organisations must make sure that such data is kept private and shared only with permission from patients or legal authorities.

Algorithmic Bias: If AI systems are trained on incomplete or unrepresentative datasets, they may yield biased results. Reducing algorithmic bias is crucial to ensuring fair healthcare in a diverse nation like India.

Fairness: AI should give everyone access to fair, nondiscriminatory healthcare. Equal access to AI technologies, ongoing monitoring, and comprehensive datasets are necessary for fairness.

Accountability: Policymakers, hospitals, AI developers, and healthcare professionals must continue to take responsibility for the ethical and safe application of AI. When AI-assisted judgments cause harm to patients, it is crucial to have clear responsibilities.

Trust: For AI to be successfully implemented in healthcare, public trust is essential. Building trust in AI systems requires transparency, human oversight, robust data protection, and efficient regulation.

6. Regulatory Challenges of AI in Healthcare

The rapid adoption of Artificial Intelligence (AI) in healthcare has outpaced the development of an appropriate regulatory framework in India. Although existing laws relating to data protection, information technology, and medical ethics provide partial governance, they do not comprehensively regulate AI-based healthcare systems. The absence of clear and uniform regulations creates uncertainty regarding the development, deployment, oversight, and accountability of AI technologies in healthcare¹⁷.

Lack of Comprehensive AI Legislation: There isn't a specific law governing AI in healthcare in India. Only a few facets of AI are covered by current laws and regulations, which do not

¹⁶ Rabaï Boudherhem, Shaping the future of AI in healthcare through ethics and governance, HSSC, 1, 5, (2024)

fully address concerns like liability, explainability, responsibility, and patient protection.

Fragmented Regulation: The MoHFW, NMC, ICMR, MeitY, NITI Aayog, and CDSCO are among the authorities that oversee AI governance. This disjointed approach results in inconsistent regulatory scrutiny and multiple tasks.

Lack of AI Standards: For the development, testing, validation, and oversight of healthcare AI systems, India lacks consistent standards. To guaranty patient safety, precise guidelines on cybersecurity, bias, accuracy, and transparency are crucial.

AI Approval: There is no dedicated approval mechanism for many AI-based healthcare systems. Since AI models evolve over time, they require continuous validation, regulatory oversight, and post-market monitoring.

Regulatory Sandboxes: Regulatory sandboxes allow AI technologies to be tested under regulatory supervision before large-scale deployment. They encourage innovation while ensuring safety, effectiveness, and ethical compliance.

Cross Border Data Governance: AI in healthcare frequently entails the international transfer of medical data for cloud-based services and research. To guaranty data security, regulatory compliance, and patient privacy protection during overseas data transfers, India needs explicit regulations.

7. Comparative Analysis

The way AI is governed in healthcare varies significantly across jurisdictions. While some nations have enacted legally binding laws, others rely on industry-specific rules and moral standards. Analysing these strategies offers insightful information for creating a successful AI governance structure in India.

7.1 European Union

The European Union has established one of the world's most comprehensive regulatory frameworks through the Artificial Intelligence Act (AI Act), which adopts a risk-based approach. AI systems used in healthcare are generally classified as high-risk and are subject to stringent requirements, including risk management, high-quality datasets, transparency, human oversight, and post-market monitoring. In addition, the European Health Data Space (EHDS)¹⁷ facilitates the secure use of health data for research and AI innovation while maintaining strong privacy protections under the GDPR. This framework seeks to balance innovation with patient

¹⁷ EUROPEAN COMMISSION, https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en, (last visited Sep 04, 2026).

safety and fundamental rights.

7.2 United States

The United States controls AI in healthcare primarily through the Food and Drug Administration (FDA)¹⁸, particularly if AI acts as Software as a Medical Device (SaMD). The FDA employs a Total Product Lifecycle (TPLC) strategy that prioritises post-market surveillance, real-world performance, ongoing monitoring, and pre-market assessment. Despite the lack of a comprehensive AI law, the U.S. regulatory paradigm concentrates on sector-specific regulation to guaranty the efficacy and safety of AI-enabled medical products.

7.3 United Kingdom

The Medicines and Healthcare Products regulation Agency (MHRA) of the United Kingdom uses a principles-based regulation approach. AI-enabled medical devices are subject to regulations that prioritise human oversight, explainability, openness, and patient safety. Along with fostering responsible AI implementation inside the National Health Service (NHS), the UK also fosters innovation through regulatory guidelines, Good Machine Learning Practice, and AI testing environments.

7.4 Singapore

Singapore has created a framework for AI governance that is fair and favourable to innovation. The Artificial Intelligence in Healthcare Guidelines (AIHGle), released by the Ministry of Health (MOH) and the Health Sciences Authority (HSA)¹⁹, place a strong focus on human monitoring, responsibility, openness, and patient safety. Singapore is one of the top jurisdictions in responsible AI governance within the healthcare industry thanks to its robust data protection regulations and governmental support for innovation.

7.5 Lessons for India

Clear legislation, risk-based regulation, robust data protection, human oversight, and ongoing monitoring are all necessary for effective AI governance, as the comparative analysis shows. The United States emphasises lifecycle regulation of AI-enabled medical devices, the United Kingdom emphasises principles-based governance, Singapore shows how innovation can be

¹⁸ U.S FOOD AND DRUG ADMINISTRATION, <https://www.fda.gov/>, (last visited Sep 04, 2026)

¹⁹ MINISTRY OF HEALTH SINGAPORE, <https://www.hcsa.gov.sg/licensable-healthcare-services/moh-mhc-cir-0024-2026-updated-moh-artificial-intelligence-in-healthcare-guidelines--aihgle-2-0-/moh-mhc-cir-0024-2026-updated-moh-artificial-intelligence-in-healthcare-guidelines--aihgle-2-0/> (last visited Sep 05, 2026)

combined with ethical precautions, and the European Union offers a strong legislative approach. By enacting specific AI laws for healthcare, setting regulatory standards for AI systems, bolstering clinical validation and post-market monitoring, guaranteeing accountability and transparency, and developing a coordinated governance framework that upholds patient rights while promoting technological innovation, India can benefit from these strategies.

8. Building an Effective AI Governance Framework in India

India requires a comprehensive and future-oriented governance framework to ensure the safe, ethical, and accountable use of Artificial Intelligence (AI) in healthcare. This framework should include a dedicated AI healthcare law that clearly defines the responsibilities of healthcare professionals, hospitals, AI developers, and regulatory authorities. A risk-based regulatory approach should be adopted, subjecting high-risk AI applications used in diagnosis and treatment to stricter oversight, clinical validation, and continuous monitoring. AI should function only as a decision-support tool, with mandatory human oversight ensuring that final medical decisions remain with qualified healthcare professionals. The framework should also promote explainable AI, enabling both clinicians and patients to understand the basis of AI-assisted decisions and strengthening accountability. Before deployment, AI systems should undergo independent certification to ensure their safety, accuracy, and reliability. In addition, strong data governance supported by robust consent mechanisms and compliance with the Digital Personal Data Protection Act, 2023, is essential to safeguard patient information. Given the growing threat of cyberattacks, uniform cybersecurity standards must be implemented to protect digital health infrastructure and sensitive medical data. India should also consider establishing an independent AI regulatory authority to oversee the approval, monitoring, and compliance of AI systems in healthcare. Finally, the governance framework should adopt a patient-centric approach by recognising patients' rights to privacy, informed consent, transparency regarding AI use, meaningful human review, and access to effective legal remedies in cases of AI-related harm. Such a balanced framework would promote innovation while ensuring patient safety, accountability, and public trust in AI-enabled healthcare.

9. Conclusion

Artificial Intelligence has the potential to transform India's healthcare sector by improving diagnostic accuracy, enhancing clinical decision-making, accelerating drug discovery, and expanding access to quality healthcare services. However, there are serious ethical, legal, and

regulatory issues with patient privacy, informed consent, medical negligence, algorithmic bias, transparency, accountability, and cybersecurity that are brought up by its growing incorporation into healthcare. The Digital Personal Data Protection Act, 2023, the Ayushman Bharat Digital Mission, the ICMR Ethical Guidelines, and NITI Aayog's Responsible AI initiatives are just a few of the significant legislative and policy measures that India has introduced. However, these frameworks are still disjointed and do not fully regulate AI in healthcare.

The comparative research shows that countries like Singapore, the United States, the United Kingdom, and the European Union have implemented organised systems that strike a compromise between patient safety and accountability and technology innovation. By creating a specific legal framework that includes risk-based regulation, robust data governance, required human monitoring, explainable AI, and efficient regulatory oversight, India may learn a lot from these models. In conclusion, AI should enhance rather than take the place of medical professionals' knowledge and discretion. Building public trust and facilitating the ethical and sustainable application of AI in India's healthcare system require a robust regulatory structure that protects patient rights, guarantees accountability and transparency, and encourages responsible innovation.

