

THE LEGAL CHALLENGES OF AI IN HEALTHCARE: CYBER-LEGAL ANALYSIS OF LIABILITY AND SYSTEMIC VULNERABILITIES UNDER INDIAN LAW

AUTHOR – BALASUBRAMANIAN K.V., STUDENT AT CYBER SPACE LAW AND JUSTICE DEPARTMENT, SCHOOL OF EXCELLENCE IN LAW, THE TAMILNADU DR. AMBEDKAR LAW UNIVERSITY

BEST CITATION – BALASUBRAMANIAN K.V, THE LEGAL CHALLENGES OF AI IN HEALTHCARE: CYBER-LEGAL ANALYSIS OF LIABILITY AND SYSTEMIC VULNERABILITIES UNDER INDIAN LAW, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (9) OF 2026, PG. 747-756, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT

Artificial Intelligence (AI) is transforming healthcare through applications such as diagnostics, robotic surgery, predictive analytics, telemedicine, drug discovery, and patient monitoring. While AI improves efficiency, accuracy, and accessibility, particularly in developing countries like India, it also creates significant legal, ethical, constitutional, and cybersecurity concerns. This study critically examines the challenges posed by AI-driven healthcare systems through a cyber-legal and comparative analysis. It evaluates the adequacy of existing Indian laws, including the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, and the National Medical Commission Act, 2019, along with ethical guidelines issued by the Indian Council of Medical Research. The paper further explores constitutional principles such as privacy, dignity, informed consent, equality, and the right to health under Article 21, supported by landmark judgments including Justice K.S. Puttaswamy v. Union of India. It identifies regulatory gaps concerning liability, algorithmic bias, cybersecurity, accountability, and data protection, while comparatively analysing AI governance models in the European Union, United States, China, Japan, Canada, and Singapore. The study concludes that India requires comprehensive AI-specific healthcare legislation balancing innovation with constitutional and ethical safeguards.

INTRODUCTION

The integration of Artificial Intelligence (AI) into the healthcare ecosystem is fundamentally transforming the paradigms of diagnostics, predictive analytics, robotic surgery, and personalized treatment. By augmenting human clinical judgment with algorithmic precision, AI promises to democratize healthcare delivery and enhance patient outcomes. However, this rapid technological assimilation significantly outpaces existing legal frameworks, which are predicated on human-centric professional standards, individual autonomy, and traditional concepts of negligence. In India, the absence of a dedicated AI-specific legislative framework has necessitated reliance on a fragmented

regulatory mosaic, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Consumer Protection Act, 2019, and the Medical Devices Rules, 2017. This regulatory reliance creates a distinct "accountability vacuum," particularly in high-risk clinical sectors. As AI systems evolve from passive diagnostic assistants into semi-autonomous decision-makers, they challenge the foundational principles of medical jurisprudence. The shift from human-driven clinical judgment—governed by the *Bolam* and *Bolitho* standards of "responsible medical opinion"—to algorithmic outputs introduces profound complexities regarding liability, informed consent, and due process. Furthermore, the reliance on opaque, proprietary

"black box" algorithms complicates the patient's right to transparent care, a critical component of the right to health under Article 21 of the Indian Constitution. This research project critically evaluates these challenges, positioning AI not merely as a clinical tool, but as a complex socio-technical platform that demands novel regulatory strategies. By examining the tension between technological innovation and the preservation of patient rights, this study explores whether established doctrines—such as "commercial wisdom" or federal preemption—can withstand the unique risks posed by adaptive AI. Ultimately, it argues that in the absence of a comprehensive legislative structure, the judiciary must adapt existing common-law principles of product liability and negligence to prevent an "accountability gap." As AI assumes a central role in India's digital health infrastructure, the synthesis of technological transparency and rigorous legal oversight becomes essential to ensuring that the pursuit of innovation does not compromise the fundamental right to life and bodily integrity.

Research Questions

1. Who is liable for AI-related medical errors in healthcare?
2. Are existing Indian laws sufficient to regulate AI in healthcare?
3. How do cybersecurity risks in AI systems affect patient rights and liability?
4. Can traditional medical negligence principles apply to AI-assisted healthcare?
5. What legal and regulatory reforms are needed for AI governance in healthcare?

Research Hypothesis

The existing Indian legal framework is inadequate to address the liability and cybersecurity challenges posed by AI in healthcare, necessitating a specialized and integrated regulatory regime.

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) refers to computer systems capable of performing tasks that

normally require human intelligence, including learning, reasoning, decision-making, and problem-solving. The term was first introduced by John McCarthy, who described AI as the science and engineering of creating intelligent machines. AI is generally classified into Narrow AI, General AI, and Super AI based on capability, and into Reactive Machines, Limited Memory, Theory of Mind, and Self-Aware AI based on functionality. Key AI models include Machine Learning, Deep Learning, and Generative AI. In healthcare, most current applications rely on Narrow AI and Limited Memory systems for data-driven decision support and clinical assistance. AI is increasingly used across healthcare for diagnosis, treatment planning, patient monitoring, and administrative management. Reactive and Limited Memory AI systems are widely employed in medical imaging, disease prediction, electronic health records, and healthcare administration. Machine Learning and Deep Learning models assist in detecting diseases such as cancer, tuberculosis, and cardiac disorders, while Generative AI supports medical documentation, drug discovery, and virtual healthcare assistance. Emerging autonomous systems are being integrated into robotic surgery and intensive care monitoring. In India, AI applications are expanding through digital health initiatives and large healthcare datasets, although concerns relating to transparency, bias, cybersecurity, and legal accountability remain significant.

MODERN HEALTHCARE IN INDIA

India's healthcare sector is undergoing a rapid digital transformation, shifting from a reactive, hospital-centric model to a proactive, technology-driven ecosystem supported by government initiatives like the Ayushman Bharat Digital Mission (ABDM) and platforms such as e-Sanjeevani. This evolution integrates advanced technologies like Artificial Intelligence (AI), Machine Learning (ML), and wearable devices to enhance diagnostic accuracy, streamline operations, and democratize access to care, particularly for rural and underserved populations. While these innovations offer

unprecedented opportunities to improve clinical outcomes and resource allocation, they also introduce significant challenges related to data privacy, algorithmic bias, and the need for clear accountability frameworks for AI-driven clinical decisions. Consequently, the successful integration of these digital solutions requires a balanced approach that combines robust legal safeguards, such as those envisioned in the Strategy for AI in Healthcare (SAHI), with ethical oversight and inclusive policy frameworks to ensure an equitable, future-ready healthcare system.

ADOPTION OF AI IN HEALTHCARE IN INDIA

India has actively embraced Artificial Intelligence (AI) in healthcare through policy initiatives, ethical frameworks, public health programs, and private-sector innovation. The adoption process is guided by a combination of governance mechanisms, technological platforms, and healthcare applications aimed at improving accessibility, efficiency, and quality of care.

1. **ICMR Ethical Guidelines for Application of AI in Biomedical Research and Healthcare (2023)** provide India's first dedicated ethical framework for healthcare AI. The guidelines emphasize transparency, accountability, privacy, fairness, safety, informed consent, and human oversight. Through the Human-in-the-Loop approach, they ensure that AI assists healthcare professionals without replacing clinical judgment.
2. **The Strategy for Artificial Intelligence in Healthcare for India (SAHI), 2026** serves as India's comprehensive policy framework for healthcare AI governance. It promotes trust, transparency, accountability, fairness, and patient safety while adopting a lifecycle approach covering AI development, deployment, monitoring, and risk management.
3. Complementing SAHI is the **Benchmarking Open Data Platform for Health AI (BODH), 2026**, developed by the National Health Authority and IIT Kanpur. BODH provides independent validation and benchmarking of healthcare AI systems through a privacy-preserving federated architecture. It evaluates AI tools for accuracy, fairness, explainability, safety, and regulatory compliance.
4. Together, **SAHI and BODH** form the foundation of India's AI healthcare governance ecosystem. While SAHI establishes policy principles and accountability standards, BODH operationalizes these principles through technical testing, fairness assessment, and continuous monitoring.
5. The Government of India has also established **Centres of Excellence for Artificial Intelligence** at institutions such as AIIMS Delhi, PGIMER Chandigarh, and AIIMS Rishikesh. These centres promote research, innovation, and development of indigenous AI solutions tailored to Indian healthcare needs.¹⁴⁰⁵
6. AI is increasingly being applied in **public health surveillance** through initiatives such as **Media Disease Surveillance (MDS)**, which uses AI to monitor digital sources and identify disease outbreaks in real time, enabling faster public health responses.¹⁴⁰⁶
7. In the field of **telemedicine**, the AI-enabled **Clinical Decision Support System (CDSS)** integrated into the eSanjeevani platform assists doctors with diagnostic and treatment recommendations, improving healthcare delivery in remote and underserved regions.¹⁴⁰⁷
8. AI has also been deployed in disease-specific programs. Tools such as **Cough Against TB** and **Prediction of Adverse TB Outcomes** support tuberculosis detection, risk assessment, and treatment monitoring. Similarly, diagnostic platforms such as **DeepCXR** and **MadhuNetrAI** assist in chest X-

¹⁴⁰⁵ Shri Dharmendra Pradhan announces 3 Centres of Excellence in AI in Healthcare, Agriculture and Sustainable Cities dt. 15.10.2024

¹⁴⁰⁶ Union Minister of State for Health and Family Welfare Smt. Anupriya Patel participates in a Session on "Innovation to Impact: AI as a Public Health

Game-Changer" at India AI Impact Summit 2026, Highlights AP's Transformative Role in Public Health dt. 17.02.2026

¹⁴⁰⁷ <https://www.digitalindia.gov.in/initiative/esanjeevani/>

ray analysis and diabetic retinopathy screening, expanding access to specialized healthcare services.¹⁴⁰⁸

9. The **IndiaAI Application Development Initiative** further promotes innovation in areas such as cancer detection, radiology, wearable technologies, and neuroinformatics by encouraging collaboration among government institutions, researchers, and startups.¹⁴⁰⁹
10. The private sector has played an equally significant role. Companies such as Qure.ai, Cloudphysician, Thermalytix, EkaCare, and Plus91 have developed AI-driven solutions for diagnostics, ICU monitoring, radiology, and digital health management.

CONSTITUTIONAL DIMENSIONS OF AI IN HEALTHCARE

1. The deployment of Artificial Intelligence in healthcare must also be examined through the constitutional framework of Article 21 of the Constitution of India. The Supreme Court has consistently held that the Right to Health forms an integral part of the Right to Life and Personal Liberty. In *Paschim Banga Khet Mazdoor Samity v. State of West Bengal*¹⁴¹⁰, the Court recognized the State's obligation to provide adequate medical facilities and access to healthcare. AI technologies possess the potential to strengthen this constitutional mandate by improving diagnostic accuracy, reducing healthcare disparities, and expanding access to medical services. However, unsafe, biased, or inadequately regulated AI systems may adversely affect healthcare outcomes, thereby raising constitutional concerns regarding the protection of health and life under Article 21.
2. The *Puttaswamy judgment*¹⁴¹¹ further recognized human dignity as a foundational constitutional value

underlying the right to privacy. In the healthcare context, dignity requires that patients retain meaningful control over personal information and are treated as autonomous individuals rather than merely sources of data for algorithmic systems. AI applications that engage in excessive profiling, opaque decision-making, or unauthorized data sharing may undermine patient dignity by reducing individuals to statistical categories and limiting their ability to make informed choices regarding medical treatment. Consequently, the protection of dignity becomes an essential component of AI governance in healthcare.

CORE LEGAL ISSUES OF AI IN HEALTHCARE IN INDIA

A. LIABILITY AND ACCOUNTABILITY GAP IN AI HEALTHCARE

The integration of Artificial Intelligence (AI) into healthcare has transformed diagnosis, treatment planning, disease prediction, and clinical decision-making. AI systems are increasingly used to interpret radiological images, recommend treatment options, and assist healthcare professionals in delivering medical services. While these technologies improve efficiency and accuracy, they create a significant legal challenge regarding liability when AI-assisted decisions result in patient harm. Traditional medical negligence law was developed on the assumption that healthcare decisions are made by human professionals. AI-assisted healthcare introduces multiple actors into the decision-making process, including doctors, hospitals, software developers, and technology providers. When an AI-generated recommendation causes injury, determining who should bear legal responsibility becomes difficult. This uncertainty is commonly referred to as the "liability gap" or "accountability gap."

¹⁴⁰⁸ Steps taken to include AI-based diagnostic tools in healthcare dt. 05.12.2025

¹⁴⁰⁹ Transforming Healthcare Delivery Through Artificial Intelligence dt. 13.02.2026

¹⁴¹⁰ AIR 1996 SC 2426

¹⁴¹¹ AIR 2018 SC 237

Under existing Indian law, AI systems do not possess legal personality and therefore cannot be sued or punished. Liability must therefore be attributed to human or institutional actors involved in the deployment and use of AI. Clinicians remain responsible for patient care, hospitals may incur institutional liability for deploying unsafe technologies, and developers may face liability for defective algorithms or inadequate testing.

The leading authority on medical negligence in India remains the Supreme Court decision in *Jacob Mathew v. State of Punjab*¹⁴¹². The Court adopted the Bolam Test and held that a doctor is not negligent if he acts in accordance with a responsible body of professional medical opinion. The judgment emphasized that mere errors of judgment do not constitute negligence. The application of this principle becomes difficult in AI-assisted healthcare. The Bolam Test¹⁴¹³ assumes that a doctor exercises independent professional judgment. However, many AI systems operate as "black boxes" whose reasoning cannot easily be understood even by developers. If a clinician relies upon an AI-generated diagnosis that later proves incorrect, courts may face difficulty in determining whether the doctor exercised independent judgment or merely followed the algorithm. Consumer protection law also provides an important basis for liability. In *Indian Medical Association v. V.P. Shantha*¹⁴¹⁴, the Supreme Court held that medical services fall within the scope of consumer protection legislation. Consequently, patients may seek compensation for deficiencies in healthcare services. In AI-related disputes, this principle enables patients to pursue remedies against healthcare providers. However, the judgment does not resolve whether liability should rest upon the doctor, hospital, or AI developer. Institutional liability assumes particular importance in AI healthcare. In *Spring Meadows Hospital v. Harjol Ahluwalia*¹⁴¹⁵, the Supreme Court held hospitals

vicariously liable for negligence committed within their healthcare system. The Court recognized that hospitals owe an extended duty of care to patients. Applying this principle to AI, hospitals may be liable where they deploy unvalidated AI systems, fail to train staff regarding AI limitations, or neglect adequate supervision mechanisms. The National Medical Commission Act, 2019 plays an indirect but significant role in AI-assisted healthcare. The Act regulates professional standards, ethics, and medical practice in India. Even where AI tools assist diagnosis or treatment, registered medical practitioners remain responsible for maintaining professional standards prescribed by the NMC. Consequently, AI cannot replace the statutory obligations of medical practitioners, and clinicians remain accountable for exercising independent judgment while using AI-based systems.

The Supreme Court's decision in *Managing Director, Kamineni Hospitals v. Peddi Narayana Swami*¹⁴¹⁶ further reinforced institutional accountability by emphasizing that hospitals cannot avoid responsibility for failures occurring within their healthcare ecosystem. Although not an AI case, its reasoning supports extending liability to AI-assisted healthcare environments. At present, India lacks a dedicated statutory framework governing AI-related medical liability. Existing disputes must therefore be resolved through principles of negligence, consumer protection, vicarious liability, and tort law. To address these concerns, the Ministry of Health introduced the Strategy for Artificial Intelligence in Healthcare (SAHI) and the Benchmarking Open Data Platform for Health AI (BODH). SAHI adopts a role-based accountability framework under which developers are responsible for design and validation, hospitals for governance and monitoring, and clinicians for final clinical decisions. BODH complements this framework through independent testing, benchmarking, and safety validation of AI systems. Despite

¹⁴¹² AIR 2005 SC 3180

¹⁴¹³ 1957 1 WLR 583

¹⁴¹⁴ AIR 1996 SC 550

¹⁴¹⁵ AIR 1998 SC 1801

¹⁴¹⁶ 2025 INSC 527

these developments, SAHI and BODH currently function as governance frameworks rather than binding legislation. Consequently, the liability gap remains one of the most significant unresolved legal challenges in AI healthcare regulation in India.

B. CYBERSECURITY AND SYSTEMIC VULNERABILITIES IN AI HEALTHCARE

AI healthcare systems operate through interconnected networks, cloud infrastructures, electronic health records, and machine-learning models. While these technologies improve healthcare delivery, they expose institutions to significant cybersecurity risks that may directly affect patient safety. Healthcare organizations possess highly valuable personal information, including medical records, biometric identifiers, genetic data, and treatment histories. Consequently, they have become attractive targets for cybercriminals. A successful cyberattack may compromise patient confidentiality, disrupt healthcare services, and interfere with clinical decision-making. The primary legal framework governing cybersecurity is the Information Technology Act, 2000. Section 43A imposes liability upon body corporates that fail to implement reasonable security practices while handling sensitive personal data. Hospitals and healthcare providers deploying AI systems must therefore adopt adequate cybersecurity measures to prevent unauthorized access and misuse of patient information. The Digital Personal Data Protection Act, 2023 further requires healthcare institutions, acting as Data Fiduciaries, to implement reasonable safeguards against personal data breaches. Failure to comply may attract substantial penalties. The seriousness of these risks became evident during the widely reported 2024 breach involving Star Health and Allied Insurance, where sensitive health information was allegedly exposed.¹⁴¹⁷ Although not directly related to AI, the incident highlighted the legal, financial, and reputational

consequences of cybersecurity failures in the healthcare sector. AI systems face additional vulnerabilities not found in conventional software. Data poisoning occurs when attackers manipulate training datasets, causing AI systems to learn inaccurate patterns. Similarly, adversarial attacks involve subtle modifications to medical inputs that produce incorrect diagnostic outputs. Such attacks may cause AI systems to misclassify diseases or generate unsafe recommendations. These vulnerabilities complicate traditional concepts of causation and liability. Harm may result not from a doctor's error but from manipulation of an AI model by third parties. Consequently, responsibility may potentially extend to developers, hospitals, cybersecurity personnel, and technology vendors. Ransomware represents another major threat. By encrypting hospital data and disabling critical systems, ransomware attacks can interrupt emergency services, delay treatment, and jeopardize patient safety. In AI-driven healthcare environments, the consequences may be particularly severe because many clinical processes depend upon continuous access to digital systems. Recognizing these risks, SAHI and BODH emphasize cybersecurity audits, continuous monitoring, validation, and incident reporting. However, India still lacks AI-specific cybersecurity legislation comparable to the risk-based regulatory approach adopted in other jurisdictions. Consequently, cybersecurity governance in AI healthcare continues to rely primarily upon the IT Act, DPDP Act, and general negligence principles.

C. DATA PROTECTION AND PRIVACY RISKS IN AI HEALTHCARE

AI systems depend upon vast quantities of patient data, including medical records, diagnostic reports, biometric identifiers, and genetic information. While such data enables advanced healthcare applications, it also raises significant concerns regarding privacy, consent, and data protection.¹⁴¹⁸ Health information is

¹⁴¹⁷ A Cautionary Tale: Lessons from the Star Health Insurance Data Breach _ Heer Chheda

¹⁴¹⁸ Addressing Bias, Privacy, Security, and Patient Autonomy in Artificial Intelligence (AI)-Driven Healthcare: A Review of Current Guidelines _ Shruti Singh, Prashant K. Singh, Rajesh Kumar, Riya Vaidyar

among the most sensitive forms of personal data because it reveals intimate details about an individual's physical and mental condition. Unauthorized disclosure may result in discrimination, social stigma, insurance exclusion, and identity theft. The Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 provide the principal legal safeguards. Under the DPDP Act, hospitals function as Data Fiduciaries and must process personal data lawfully, securely, and for specified purposes. Consent must be free, informed, and specific. A significant challenge arises because AI systems often require secondary use of data. Information collected for treatment may subsequently be used for training algorithms or improving AI models. Such practices raise concerns regarding purpose limitation and informed consent, particularly where patients are unaware of the extent of AI processing. The constitutional foundation for privacy protection was established in Justice K.S. Puttaswamy v. Union of India. The Supreme Court unanimously recognized privacy as a fundamental right under Article 21 and emphasized informational autonomy. The Court held that any interference with privacy must satisfy the tests of legality, necessity, and proportionality. The principles laid down in Puttaswamy have direct implications for AI healthcare. Healthcare institutions and AI developers must justify data collection, ensure transparency, and provide meaningful control over personal information. AI systems that engage in excessive collection or opaque data-sharing practices may violate both statutory obligations and constitutional protections. Privacy concerns also arise from machine-learning techniques themselves. Advanced models may enable model inversion attacks or membership inference attacks, through which sensitive information can potentially be reconstructed or inferred from AI outputs. These risks demonstrate the limitations of traditional data protection frameworks in addressing AI-specific challenges. To mitigate these concerns, privacy-preserving technologies such as

federated learning have emerged. Rather than transferring raw patient data to centralized servers, federated learning allows AI models to be trained locally while keeping sensitive information within institutional control. BODH incorporates this privacy-by-design approach by enabling evaluation and benchmarking without requiring transfer of raw patient data. Through federated learning and cryptographic audit mechanisms, BODH seeks to balance innovation with privacy protection while supporting compliance with the DPDP Act.

D. ALGORITHMIC BIAS AND ETHICAL CONCERNS IN AI HEALTHCARE

Algorithmic bias represents a significant ethical and legal challenge in AI healthcare. Because AI systems learn from historical datasets, they may replicate and amplify existing inequalities reflected in those datasets. Biased AI can therefore produce discriminatory outcomes while appearing objective. One of the primary causes of algorithmic bias is unrepresentative training data. Many healthcare AI models are trained using datasets that inadequately reflect India's demographic diversity. As a result, systems may perform accurately for some populations while producing less reliable outcomes for others. Such bias has constitutional implications under Article 14 of the Constitution, which guarantees equality before the law and equal protection of laws. If AI systems deployed in public healthcare consistently disadvantage particular demographic groups, questions of discrimination and unequal treatment may arise. The ethical principles developed by the Indian Council of Medical Research emphasize fairness, transparency, accountability, safety, and human oversight. These principles require AI to augment rather than replace clinical judgment. Transparency remains particularly important because many AI systems function as black boxes. Patients and clinicians may be unable to understand the reasoning behind algorithmic recommendations, thereby undermining trust and accountability. To address these concerns, BODH incorporates

fairness benchmarking and demographic performance testing. AI systems are evaluated across different population groups to identify disparities before deployment. Similarly, SAHI promotes fairness audits, explainability requirements, and continuous monitoring to ensure equitable healthcare outcomes. Algorithmic bias therefore raises concerns extending beyond technical performance. It engages constitutional principles of equality, ethical obligations of fairness, and broader questions regarding the responsible deployment of AI in healthcare. By embedding fairness and transparency within AI governance frameworks, India seeks to ensure that technological innovation does not come at the cost of equity and justice.

COMPARATIVE ANALYSIS: AI IN HEALTHCARE LAWS

The regulatory landscape for AI in healthcare as of May 2026 reflects a global shift toward practical governance and clinical safety.

1. The **United States** follows a decentralized and sector-specific approach. The FDA regulates AI-enabled Software as a Medical Device (SaMD), while HIPAA governs health data privacy. Several states have introduced laws requiring transparency, informed consent, and human oversight in AI-assisted healthcare.
2. The **UK** adopts an innovation-friendly framework emphasizing ethical governance and clinician oversight. Healthcare AI is regulated by the MHRA, while data protection is governed by the UK GDPR and the Data Protection Act 2018. Human-in-the-loop decision-making remains a core regulatory principle.
3. The **European Union** has established one of the most comprehensive AI frameworks through the EU AI Act. Most healthcare AI systems are classified as high-risk and must comply with strict requirements relating to transparency, data governance, human oversight, and

conformity assessments, alongside GDPR protections for health data.

4. China follows a centralized and state-driven regulatory model. AI healthcare systems are subject to extensive government oversight, including algorithm registration, security assessments, ethics reviews, and data localization requirements under the PIPL and Data Security Law. The framework prioritizes national security and public safety.
5. **India** currently regulates healthcare AI through existing laws such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. Governance initiatives such as SAHI and BODH promote transparency, fairness, and accountability, although they presently operate as non-binding frameworks.
6. **Japan** follows a trust-based and human-centric regulatory approach. The PMDA regulates AI medical devices, while privacy protection is ensured under the Act on the Protection of Personal Information (APPI). The framework emphasizes ethical innovation, transparency, and public trust in healthcare technologies.
7. **Canada** regulates healthcare AI through Health Canada's medical device framework and privacy protections under PIPEDA. The country focuses on responsible AI deployment, risk management, and safeguarding vulnerable populations while encouraging innovation through institutional governance mechanisms.
8. **Singapore** adopts a pragmatic, risk-based model that combines regulatory oversight with flexible governance. The Health Sciences Authority regulates healthcare AI, while the Model AI Governance Framework provides guidance on ethical deployment, transparency, accountability, and safe

integration into public healthcare systems.

Among these jurisdictions, the European Union and China have adopted the most comprehensive regulatory frameworks, while the United States and Canada rely on sector-specific regulation. Japan and Singapore emphasize ethical governance and innovation, whereas India currently follows a policy-driven approach through existing legislation and voluntary governance frameworks, highlighting the need for a dedicated AI healthcare regulatory regime.

LEGISLATIVE RECOMMENDATIONS FOR HEALTH AI IN INDIA

1. Propose legislative amendments specifying allocation of liability among the developers, hospitals, and clinicians to resolve ambiguity in medical malpractice and consumer protection laws and establish the "chain of liability".
2. Propose legislative amendment formalizing a regulatory pathway through Central Drugs Standard Control Organization for AI software as a medical device. It should replace existing voluntary guidelines for pre-market safety, clinical validation, and algorithmic transparency certification for high-risk diagnostic applications.
3. Ensure that standards for benchmarking and transparency, currently recommended by SAHI and BODH, are legally mandated requirements for any AI systems operating in high-risk clinical settings.
4. Form an authoritative central committee for licensing high-risk AI applications, undertaking technical audits for ensuring safety, and conducting investigations in cases where adverse incidents result from the use of algorithms.
5. Enforce a legal requirement for AI-driven healthcare organizations to undertake independent periodic audit of their cybersecurity practices specifically pertaining to adversarial attacks,

algorithmic manipulation, and data poisoning.

6. Define legal concept of "AI-Specific Informed Consent" within the DPDP act framework. It is essential to ensure that patients are explicitly informed about the use of their clinical data in model training or research and are made aware of an easy method of withdrawal.

These recommendations target the transition of India's current policy-driven approach into a robust, enforceable legal structure that protects patients while ensuring the safe integration of artificial intelligence into the national healthcare infrastructure.

CONCLUSION

AI is a transformative force in Indian healthcare, offering solutions to professional shortages and inequitable access. However, its integration introduces complex challenges—specifically regarding liability, cybersecurity, data privacy, and algorithmic bias—that current legal doctrines were not designed to navigate. While foundational rulings like *Puttaswamy* and *Jacob Mathew* offer guidance, they are insufficient to address the unique opacity and autonomy of AI systems. Voluntary governance initiatives like SAHI and BODH are positive steps but lack the force of binding legislation. To fully realize AI's potential, India must adopt a comprehensive regulatory framework that balances rapid innovation with robust accountability, fairness, and constitutional protections. Such a framework is essential to safeguarding patient rights and public trust, ensuring that AI remains a tool for equitable progress within India's healthcare system.

REFERENCES

Statutes and Legislations

1. Constitution of India, 1950.
2. Information Technology Act, 2000.
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

4. Digital Personal Data Protection Act, 2023.
5. Consumer Protection Act, 2019.
6. National Medical Commission Act, 2019.
7. Bharatiya Nyaya Sanhita, 2023

Government Policies, Guidelines and Frameworks

1. Ministry of Health and Family Welfare, Government of India, Strategy for Artificial Intelligence in Healthcare for India (SAHI), 2026.
2. National Health Authority (NHA), Government of India, Benchmarking Open Data Platform for Health AI (BODH) Framework, 2026.
3. Indian Council of Medical Research (ICMR), Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare, 2023.
4. NITI Aayog, National Strategy for Artificial Intelligence – #AIForAll, 2018.
5. Ministry of Electronics and Information Technology (MeitY), IndiaAI Governance Guidelines, 2025.
6. Ayushman Bharat Digital Mission (ABDM), National Health Authority, Government of India.
7. IndiaAI Mission, Ministry of Electronics and Information Technology, Government of India.

Journal Articles and Research Sources

1. "Data Breaches in Healthcare: Examining Cyber Offences and Legal Protection in India."
2. "Algorithmic Bias in Public Health AI: A Silent Threat to Equity."
3. "Addressing Algorithmic Bias in India: Ethical Implications and Pitfalls."
4. Girish Chandra Bhatt & Manoj Kumar Gopaliya, Strategic Management of Algorithmic Bias: A Review of AI-Driven Clinical Decision Support in Healthcare Organizations.

Foreign Regulatory References

1. European Union AI Act, 2024.
2. General Data Protection Regulation (GDPR), European Union.

3. U.S. Food and Drug Administration (FDA) Guidance on AI/ML-Based Software as a Medical Device (SaMD).
4. United Kingdom Medicines and Healthcare Products Regulatory Agency (MHRA) AI Regulatory Framework.
5. China Personal Information Protection Law (PIPL).
6. China Data Security Law.
7. Japan Act on the Protection of Personal Information (APPI).
8. Canada Personal Information Protection and Electronic Documents Act (PIPEDA).
9. Singapore Model AI Governance Framework.