International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Policy to Practice: Regulatory Readiness for AI-Driven Healthcare Research in India

Dr. Mukta Bhosale
Assistant Professor,
Kaveri College of Arts, Science and Commerce, Pune

https://doi.org/10.55041/ijsmt.v2i4.117

Cite this Article: Bhosale, M. (2026). Policy to Practice: Regulatory Readiness for AI-Driven Healthcare Research in India. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.117

1. Introduction

Artificial Intelligence (AI) has emerged as a transformative technology in healthcare research, enabling improved disease prediction, automated diagnostics, personalized treatment planning and biomedical discoveries. AI-based tools have demonstrated significant potential in analyzing large datasets, identifying patterns in clinical records and improving research efficiency (Topol, 2019).

India is witnessing rapid growth in AI-based healthcare research due to increased digitization of health records, government initiatives and the expansion of the digital health ecosystem. AI technologies are being used in medical imaging, drug discovery, epidemiological modeling and clinical decision support systems.

Despite these developments, regulatory and ethical frameworks governing AI-driven healthcare research remain underdeveloped. Ethical concerns such as privacy violations, algorithmic bias and lack of transparency pose challenges to safe implementation (Floridi & Cowls, 2019).

In India, the integration of AI into public health programs is accelerated by the Ayushman Bharat Digital Mission (ABDM), which provides interoperable digital health infrastructure. The Indian Council of Medical Research has issued ethical guidelines for AI applications in biomedical research, while NITI Aayog has developed strategic frameworks promoting responsible AI development. In addition, the Ministry of Electronics and Information Technology introduced the Digital Personal Data Protection Act to regulate personal data processing.

However, these initiatives primarily consist of guidelines rather than enforceable regulatory mechanisms. This study evaluates India's regulatory preparedness and identifies gaps between policy formulation and practical implementation.

2. Objectives of the Study

The study aims to:

1. Examine the existing regulatory framework for AI-driven healthcare research in India.
2. Evaluate the ethical and legal challenges associated with AI use in healthcare research.
3. Assess India's regulatory readiness for AI governance.
4. Identify gaps in the current framework.
5. Suggest policy recommendations for effective governance.

3. Research Methodology

This study uses a **doctrinal and qualitative research methodology** based on secondary data sources.

Sources include:

- Government policy documents
- Ethical guidelines
- Research articles

- International regulatory frameworks

Data was collected from academic journals, government reports and policy documents. Analytical methods were used to evaluate regulatory readiness and identify gaps.

4. AI in Healthcare Research

Artificial Intelligence (AI) has significantly transformed healthcare research by enabling the analysis of complex biomedical datasets and supporting evidence-based decision-making. Advances in machine learning and deep learning techniques have allowed researchers to process vast quantities of medical data efficiently and accurately. AI-driven tools support clinical research, disease surveillance, biomedical innovation and healthcare planning (Rajkomar et al., 2019; Topol, 2019).

AI technologies have improved the speed and accuracy of healthcare research while reducing operational costs. The use of AI in research settings has also contributed to personalized medicine and improved treatment strategies. Major applications of AI in healthcare research include disease prediction, medical imaging, drug discovery and clinical decision support systems. Applications include:

4.1 Disease Prediction

Disease prediction is one of the most significant applications of AI in healthcare research. Predictive analytics uses machine learning algorithms to analyze large datasets comprising patient demographics, clinical records, genetic information and lifestyle factors. These algorithms identify patterns that can help predict disease risks and progression.

AI-based disease prediction models enable early detection of chronic diseases such as diabetes, cardiovascular disorders and cancer. Early identification of disease risks allows researchers to develop preventive strategies and improve patient outcomes. Machine learning models can detect subtle relationships between risk factors that may not be apparent through traditional statistical methods (Rajkomar et al., 2019).

Predictive models also support public health research by identifying disease trends and potential outbreaks. AI-based epidemiological studies can help researchers understand disease patterns and develop effective intervention strategies.

According to Obermeyer and Emanuel (2016), predictive analytics has the potential to improve healthcare efficiency by identifying high-risk patients and enabling targeted interventions. However, the effectiveness of predictive models depends on data quality and representativeness.

Disease prediction systems also support precision medicine by enabling personalized risk assessment. AI-based models can recommend preventive measures tailored to individual patients based on their unique characteristics (Topol, 2019).

4.2 Medical Imaging

Medical imaging represents one of the most advanced applications of AI in healthcare research. AI-based image analysis systems use deep learning algorithms to detect abnormalities in medical images such as X-rays, computed tomography (CT) scans, ultrasound images and magnetic resonance imaging (MRI) scans. Deep learning models have demonstrated high accuracy in detecting diseases such as cancer, tuberculosis and cardiovascular conditions. These models are trained on large image datasets and can recognize patterns that are difficult for human observers to detect (Esteva et al., 2017).

AI-assisted imaging tools enable researchers to process thousands of medical images quickly and consistently. This capability improves research efficiency and supports large-scale clinical studies. Automated image analysis reduces human error and enhances the reliability of research findings. AI systems also support early disease detection by identifying small abnormalities that may not be visible during manual examination. Early detection improves treatment outcomes and contributes to better healthcare planning (Topol, 2019). In addition, AI-assisted imaging technologies enable quantitative analysis of medical images, allowing researchers to measure disease progression over time. This supports research studies and improves understanding of disease mechanisms. Validation studies are necessary to ensure that AI systems perform accurately across different patient populations.

4.3 Drug Discovery

Drug discovery is another important area where AI has significantly improved healthcare research. Traditional drug development processes are time-consuming and expensive, often taking more than a decade to bring new medicines to

market. AI technologies have accelerated this process by enabling faster identification of potential drug candidates. Machine learning algorithms can predict how different molecules will interact with biological targets, reducing the need for extensive laboratory testing (Mak & Pichika, 2019).
AI-based models can predict drug toxicity and side effects before clinical trials. This improves patient safety and reduces the likelihood of drug failure during later stages of development (Vayena et al., 2018).

4.4 Clinical Decision Support
Clinical Decision Support Systems (CDSS) represent an important application of AI in healthcare research. These systems use machine learning algorithms to analyze patient data and generate recommendations that support clinical research and treatment planning. AI-based decision support tools assist researchers in evaluating treatment outcomes and identifying effective interventions. These systems analyze large datasets containing patient histories, treatment records and clinical outcomes. Researchers can use AI tools to compare different treatment strategies and identify the most effective approaches (Rajkomar et al., 2019). AI-based CDSS also support personalized medicine by recommending treatments tailored to individual patient characteristics. Personalized treatment approaches improve patient outcomes and reduce adverse effects (Topol, 2019). However, AI-based decision support systems must be carefully evaluated to ensure accuracy and reliability. Incorrect recommendations may lead to inappropriate treatment decisions. Transparency and explainability are important requirements for clinical decision support systems (Mittelstadt, 2019).

5. Ethical Challenges in AI-Driven Healthcare Research
Artificial intelligence (AI) has significantly transformed healthcare research, despite advancements, AI-driven healthcare research raises several ethical concerns that must be addressed to ensure responsible use. Major ethical challenges include data privacy, algorithmic bias, transparency and accountability. These issues influence the reliability and acceptance of AI technologies in healthcare research (Nowakowski, 2022; Weiner et al., 2024).

5.1 Data Privacy
Data privacy is one of the most significant ethical concerns in AI-driven healthcare research. AI technologies depend heavily on large datasets, including electronic health records, genetic data and medical imaging information. The use of such sensitive data increases the risk of privacy violations and unauthorized access (Mooghali et al., 2024).
Healthcare data are highly confidential because they contain personal and medical information. Improper handling of such data can result in identity theft, discrimination and loss of patient trust. Therefore, strong data protection measures are essential to ensure ethical AI research practices (Prakash et al., 2025).
Another important aspect of data privacy is informed consent. Many individuals whose data are used for AI research may not fully understand how their data will be processed or reused. Ethical frameworks emphasize the importance of transparent consent procedures to protect patient autonomy (Weiner et al., 2024).
In addition, the use of cloud storage and digital data-sharing platforms increases the complexity of data governance. Researchers must ensure that patient information is securely stored and accessed only by authorized individuals. Techniques such as anonymization and encryption are commonly recommended to protect sensitive healthcare data (Mooghali et al., 2024).

5.2 Algorithmic Bias
Algorithmic bias is another important ethical challenge in AI-driven healthcare research. AI systems learn from historical datasets and if these datasets contain biases, the resulting algorithms may produce unfair or inaccurate outcomes (Nowakowski, 2022).
Bias in AI systems can negatively affect certain population groups which can result in unequal healthcare outcomes and reduced reliability of AI-based research findings (Prakash et al., 2025).
Algorithmic bias can arise due to several factors, including:

- Incomplete datasets
- Poor data quality
- Unbalanced training samples
- Model design limitations

To reduce bias, researchers must use diverse and representative datasets. Continuous monitoring and validation of AI models are also necessary to ensure fairness and accuracy (Weiner et al., 2024).

5.3 Transparency

Transparency is essential for maintaining trust in AI-driven healthcare research. Many AI models, especially deep learning systems, operate as complex algorithms that are difficult to interpret. This lack of interpretability is often referred to as the "black box" problem (Nowakowski, 2022). Healthcare researchers and practitioners require clear explanations of how AI systems generate results. Without transparency, it becomes difficult to verify AI-based findings or detect errors. Lack of transparency may therefore reduce confidence in AI-driven research (Mooghali et al., 2024). Transparency is also necessary for regulatory compliance. Researchers must clearly document:

- Data sources
- Algorithm design
- Testing procedures
- Performance outcomes

Proper documentation supports ethical evaluation and regulatory review of AI-based healthcare research (Prakash et al., 2025).

5.4 Accountability

Accountability refers to the assignment of responsibility for decisions influenced by AI systems. Establishing accountability in AI-driven healthcare research is challenging because multiple stakeholders are involved, including researchers, developers, healthcare institutions and regulators (Nowakowski, 2022). One major concern is determining responsibility when AI systems produce incorrect or harmful outcomes. Traditional healthcare systems assign responsibility to medical professionals, but AI-assisted research introduces new complexities (Weiner et al., 2024). Unclear accountability can lead to legal and ethical problems. It may be difficult to determine whether responsibility lies with:

- AI developers
- Research institutions
- Healthcare providers
- Regulatory agencies

These challenges highlight the importance of clearly defined governance frameworks (Prakash et al., 2025). Human supervision helps ensure ethical accountability and reduces the risks associated with automated decision-making (Mooghali et al., 2024).

Accountability mechanisms may include:

- Ethical review committees
- AI audits
- Regulatory supervision
- Documentation requirements

It is unclear who is responsible if AI systems cause harm. Developers, hospitals and researchers may share responsibility.

6. Regulatory Framework in India

6.1 Legal and Ethical Guidelines

AI governance intersects multiple legal instruments:

- *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare* in 2023:

The Indian Council of Medical Research (ICMR) has played a foundational role in shaping ethical governance for artificial intelligence (AI) in Indian healthcare research. Recognizing the rapid integration of AI tools in diagnostics, predictive analytics and public health systems, ICMR released the *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare* in 2023. These guidelines aim to ensure that technological innovation aligns with ethical standards and constitutional values, particularly the right to privacy and dignity.

The ICMR framework emphasizes four central principles: patient safety, transparency, accountability and data protection (ICMR, 2023). The ICMR guidelines recommend:

1. Preclinical testing and clinical validation of AI systems
2. Continuous post-deployment monitoring
3. Risk–benefit assessment before implementation
4. Human oversight in decision-making

AI systems should not replace clinical judgment but rather function as assistive tools under professional supervision. The guidelines stress that AI outputs must be interpreted by qualified healthcare professionals to prevent misdiagnosis or inappropriate treatment decisions (ICMR, 2023).

Furthermore, safety assessments must consider not only technical accuracy but also potential harm arising from algorithmic errors, system failures, or biased outputs. This reinforces the principle of non-maleficence in biomedical ethics.

Ethics Committees are encouraged to develop competence in reviewing AI-based protocols, particularly regarding risk assessment and algorithm validation. The responsibility for harm caused by AI systems cannot be shifted solely to technology; legal and professional accountability remains with human stakeholders (ICMR, 2023). However, these guidelines are not legally binding.

- Digital Personal Data Protection Act

The Ministry of Electronics and Information Technology enacted the Digital Personal Data Protection Act (2023). (DPDP Act), which establishes a statutory framework governing the processing of digital personal data. Given that AI-driven healthcare research relies heavily on large volumes of patient information, the Act has direct implications for research governance, ethical compliance and data stewardship. Healthcare providers, research institutions, pharmaceutical companies, digital health startups and AI developers qualify as Data Fiduciaries when they determine the purpose and means of processing personal data. Health-related information remains highly protected due to its intimate and potentially harmful nature if misused (Greenleaf, 2023). One of the foundational principles of the DPDP Act is consent-based data processing. Consent must be: free, specific, informed, unambiguous and revocable. In AI-driven healthcare research, this raises important operational considerations, but large-scale AI training models that rely on retrospective clinical datasets, obtaining fresh consent for secondary research use may pose logistical challenges. However, the Act allows certain exemptions for research, archiving and statistical purposes under prescribed conditions (Government of India, 2023). This creates a regulatory balancing mechanism—protecting patient autonomy while enabling innovation in medical research.

The DPDP Act mandates implementation of "reasonable security safeguards" and requires notification of the Data Protection Board and affected individuals in case of breaches. Complementary policies such as NITI Aayog's Responsible AI guidelines and sectoral health data policies must work in tandem with the DPDP Act to create a comprehensive governance model.

- Telemedicine Practice Guidelines

India's Telemedicine Practice Guidelines, issued on March 25, 2020, established the country's first legal framework for remote medical consultation. Released by the Ministry of Health and Family Welfare and incorporated into the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, they formalized teleconsultation standards for registered medical practitioners (RMPs). The 2020 guidelines provided legal clarity for India's telehealth sector, enabling safe, equitable access to medical care nationwide. Implementation challenges include variable internet connectivity, digital literacy gaps, and evolving integration with insurance and e-pharmacy systems.

The constitutional right to privacy (Justice K.S. Puttaswamy v. Union of India, 2017) anchors data protection norms. Ethical imperatives include bias mitigation, explainability, human oversight, and safety assurance.

7. India's Foundational AI Governance Framework

7.1 National e-Health Authority (NeHA) and Health Data Governance in India

The proposed National eHealth Authority (NeHA), conceptualized by the Ministry of Health and Family Welfare (MoHFW), Government of India, in 2015. It represented an early institutional effort to establish centralized governance for digital health infrastructure in India. NeHA was envisioned as the apex authority responsible for developing an integrated national healthcare information system and promoting standardized electronic health record (EHR) frameworks across public and private healthcare institutions (Chatterjee, 2015; Sreenivasulu et al., 2019).

Although NeHA was ultimately subsumed within later digital health reforms—particularly under the Ayushman Bharat Digital Mission (ABDM)—its conceptual design remains significant in understanding India's regulatory trajectory for AI-driven healthcare.

NeHA was proposed to perform multiple governance roles:

1. **Development of Integrated Healthcare Information Systems (IS)**
   Establishing interoperable digital health records across institutions.
2. **Standard Setting and Technical Guidance**
   Developing standards for electronic health records, data exchange protocols and cybersecurity safeguards.
3. **Promotion of Innovative Technologies**
   Guiding stakeholders in adopting emerging technologies such as artificial intelligence, big data analytics and telemedicine.

4. **Regulatory Oversight and Enforcement**

Ensuring compliance with privacy, confidentiality and security norms in health data management. NeHA was designed not merely as an advisory body but as a regulatory and standard-setting authority capable of coordinating multiple stakeholders, including hospitals, insurers, research institutions and technology firms (Bhattacharya et al., 2020).

In parallel with the NeHA initiative, the Government of India prepared a draft Health Data Privacy and Security Act (2016) in consultation with the National Law School of India University, Bengaluru. The draft legislation aimed to provide a sector-specific regulatory framework governing:

- Ownership of health data
- Privacy and confidentiality standards
- Consent mechanisms
- Security protocols
- Data sharing norms

Although the draft was submitted to the Ministry of Health and Family Welfare in July 2016, it was not enacted. Instead, broader data protection legislation later emerged in the form of the Digital Personal Data Protection Act, 2023. The absence of a dedicated health data statute means that AI-driven healthcare research currently relies primarily on general data protection laws rather than specialized sectoral regulation.

However, India still lacks a dedicated AI-health regulatory statute equivalent to the EU's risk-based AI governance model. The historical evolution from NeHA to ABDM illustrates India's gradual movement toward structured digital health governance, but AI-specific regulatory consolidation remains a work in progress.

7.2 India AI Governance Guidelines - 2025

In November 2025, the Ministry of Electronics & Information Technology (MeitY) issued the India AI Governance Guidelines. The framework adopts a principle-based, techno-legal model rather than a standalone AI statute.

- The Seven Core "Sutras",

The governance architecture rests on seven normative pillars:

1. Trust,
2. People First,

3. Innovation,
4. Fairness,
5. Accountability,
6. Understandability and
7. Safety (Ministry of Electronics & Information Technology [MeitY], 2025).

- Institutional Mechanisms

The framework establishes:

1. AI Governance Group (AIGG)

It is the apex institutional body. Its role is to provide strategic oversight, ensure coherence across governmental and regulatory actions, and help translate high-level AI principles into coordinated policy outcomes.

2. Technology & Policy Expert Committee (TPEC)

TPEC acts as a multidisciplinary advisory committee to the AI Governance Group (AIGG). It brings together specialists from fields such as AI and machine learning, law, public policy, cybersecurity, frontier technologies, and public administration to provide informed technical and regulatory guidance to the AIGG (Government of India, 2025).

3. **AI Safety Institute (AISI)**

The AI Safety Institute develops benchmarking standards, safety audits, and red-teaming mechanisms (MeitY, 2025).

7.3 Strategy for Artificial Intelligence in Healthcare for India (SAHI, 2026)

The Ministry of Health & Family Welfare introduced the Strategy for Artificial Intelligence in Healthcare for India (SAHI) in February 2026.

SAHI is structured around three interlinked goals:

1. **Enhancing Clinical Outcomes** – Leveraging AI to improve diagnostic accuracy, reduce treatment delays, and optimize resource allocation.
2. **Strengthening Public Health Surveillance** – Using predictive analytics for disease outbreaks, non-communicable disease (NCD) mapping, and health system planning.
3. **Institutionalizing Responsible AI** – Embedding ethics, safety, and accountability into healthcare AI lifecycles.

The strategy recognizes healthcare AI as a *high-impact, high-risk* domain requiring structured oversight, especially in a diverse and populous country like India. SAHI builds upon the digital backbone created under the Ayushman Bharat Digital Mission (ABDM). The strategy explicitly promotes open standards and API-based integration to prevent vendor lock-in and ensure scalability. SAHI is structured around four operational pillars:

1. **Data Governance, Quality, and Ethics**

Recognizing that AI performance depends on data quality, SAHI mandates:

- Standardized data labeling protocols
- Clinical metadata documentation
- Bias audits to detect demographic disparities
- Federated data architecture to minimize centralized data pooling

Data processing must comply with the Digital Personal Data Protection Act, ensuring lawful consent, purpose limitation, and data minimization. Ethical oversight committees at the institutional level are encouraged to review AI deployments like that of biomedical ethics boards.

2. Model Development and Clinical Validation

SAHI introduces a *tiered validation pathway*:

(a) Pre-Clinical Technical Testing

- Algorithm robustness testing
- Adversarial stress testing

- Cybersecurity evaluation

(b) Clinical Validation

- Retrospective dataset validation
- Prospective real-world pilot trials
- Multi-site validation across diverse populations

3. Integration into Clinical Workflows

A key innovation in SAHI is its focus on *implementation science*. AI tools must:

- Integrate into hospital information systems
- Align with existing diagnostic protocols
- Provide explainable outputs understandable to clinicians

The strategy discourages standalone "black box" AI tools and promotes explainability standards consistent with ethical AI principles. Capacity-building programs are proposed for:

- Clinicians (AI literacy training)
- Hospital administrators (procurement and risk assessment)
- Regulators (AI risk classification training)

4. Continuous Monitoring and Lifecycle Governance

Unlike static regulatory approvals, SAHI adopts lifecycle oversight:

- Real-world performance monitoring
- Bias re-evaluation over time
- Performance drift detection
- Mandatory reporting of adverse AI-related incidents

Mechanisms for *AI decommissioning* are in place if systems pose safety risks or are ineffective. The strategy aligns with the Digital Personal Data Protection Act and the Medical Device Rules to ensure lawful data processing and device safety compliance (Ministry of Health & Family Welfare [MoHFW], 2026). A federated data architecture protects patient privacy while enabling collaborative AI model training.

8. Institutional Readiness & Capacity Building

The *Strategy for Artificial Intelligence in Healthcare for India (SAHI), 2026),* issued by the Ministry of Health & Family Welfare, provides a sector-specific governance architecture to address high-risk AI concerns in clinical and public health settings. Rather than treating privacy, bias, and safety as abstract ethical ideals, SAHI operationalizes them through compliance mandates, institutional safeguards, and lifecycle monitoring mechanisms.

8.1. Data Privacy and Protection

SAHI integrates this requirement into AI workflows through the consent manager framework developed under the Ayushman Bharat Digital Mission (ABDM). Patients retain control over:

- Purpose-specific authorization
- Time-bound data sharing
- Revocation rights

This ensures that AI training and deployment remain legally compliant and ethically grounded (MoHFW, 2026).

8.2. Federated Learning and Data Minimization

To reduce centralization risks, SAHI promotes federated data architectures, where raw health data remain within institutional repositories while model parameters are shared for training (MoHFW, 2026). Such decentralization aligns with global privacy best practices articulated by the World Health Organization, which emphasizes safeguarding patient autonomy and confidentiality in AI systems (World Health Organization [WHO], 2021).

8. 3. Cybersecurity and Audit Trails

SAHI mandates pre-deployment cybersecurity testing and requires audit logs documenting data access and model updates (MoHFW, 2026). These safeguards mitigate adversarial attacks and unauthorized data manipulation, thereby reinforcing system integrity.

8. 4. Addressing Algorithmic Bias and Promoting Equity

Algorithmic bias poses significant risks in a socio-demographically diverse country such as India. SAHI recognizes that AI systems trained on narrow or urban-centric datasets may exacerbate health inequities.

8.5. Dataset Diversity Requirements

SAHI requires developers to demonstrate demographic representativeness in training datasets and to provide subgroup performance metrics (MoHFW, 2026). This aligns with WHO's principle of inclusiveness and equity in AI deployment (WHO, 2021).

8.6 Mandatory Bias Audits

Pre-deployment fairness assessments and periodic post-market bias audits are mandated under SAHI (MoHFW, 2026). These audits evaluate:

- Gender-based diagnostic accuracy differences
- Rural–urban performance disparities
- Socioeconomic and age-group variations

This lifecycle bias monitoring mirrors risk-based regulatory approaches seen in international frameworks such as the European Union Artificial Intelligence Act, which classifies healthcare AI as high-risk and mandates ongoing conformity assessments (European Parliament & Council, 2024).

8.7. Transparency and Explainability

Healthcare AI systems must be explainable to clinicians and patients alike. Patients must be informed when AI systems contribute to diagnostic or therapeutic decisions (MoHFW, 2026).

8.8. Documentation and Traceability

Developers must submit risk classification statements, intended-use disclosures, and validation reports. This documentation enables regulatory traceability and institutional accountability (MoHFW, 2026).

8.9. Accountability and Liability

SAHI adopts a distributed accountability framework involving:

- Developers
- Deploying institutions
- Clinical practitioners

Liability pathways are proportionate to risk classification (MoHFW, 2026). Institutional ethics committees are encouraged to evaluate AI systems similarly to biomedical research interventions. This model reflects a hybrid regulatory structure—sector-specific oversight combined with overarching digital governance under the Ministry of Electronics & Information Technology (MeitY, 2025).

8.10. Regulatory Sandboxes and Controlled Innovation

To balance innovation and safety, SAHI institutionalizes healthcare AI regulatory sandboxes, allowing supervised experimentation before large-scale deployment (MoHFW, 2026).

Such sandboxes facilitate evidence generation while minimizing systemic risk—an approach consistent with risk-proportionate regulation seen in both EU and U.S. frameworks (European Parliament & Council, 2024; FDA, 2021).

9. Conclusion

SAHI (2026) represents a structured and contextually adaptive response to AI governance challenges in Indian healthcare. By embedding privacy compliance under the Digital Personal Data Protection Act, mandating bias audits, enforcing human oversight, and instituting lifecycle monitoring, SAHI attempts to reconcile innovation with equity and patient safety.

Its success will depend on institutional capacity, enforcement rigor, and sustained public trust. Nevertheless, SAHI marks a significant advancement in operationalizing responsible AI governance within a rapidly digitizing health system. At the same time, there are no laws that take care of the criminal liabilities that may arise in due course. Specific laws will help in redressing the infringements as well as to enforce the governance framework that has been laid down by the government of India. When a doctor relies on AI-generated recommendations that result in patient harm, determining legal responsibility becomes challenging. Unlike traditional medical negligence cases—where liability is primarily attributed to the treating physician—AI-assisted decision-making involves additional actors, including software developers, technology vendors, healthcare institutions and data providers.

Under Indian law, medical professionals may be held liable under both civil and criminal frameworks: Civil liability arises under the law of torts for medical negligence. Criminal liability may arise in cases of gross negligence (Murthy, 2007). Indian courts generally apply the *Bolam test* (derived from English jurisprudence), which evaluates whether a doctor acted in accordance with a practice accepted as proper by a responsible body of medical professionals. However, the introduction of AI complicates this standard. If a doctor follows an AI recommendation that is widely adopted but later found flawed, determining whether the physician exercised "reasonable care" becomes legally ambiguous. As a result, the framework is not yet robust in addressing AI-assisted medical negligence. Another possible avenue of liability is product liability law. If AI software is classified as a "product," then developers or vendors may be liable for defects under consumer protection laws. The Consumer Protection Act, 2019 introduces product liability provisions that allow compensation claims against manufacturers and service providers for defective products or deficient services. Though SAHI holds them accountable, there are no specific laws relating to the quantum of punishment, which makes it a grey area and thus vulnerable to exploitation. Hence, to conclude SAHI seems to be very promising on paper, but for the effectiveness India also needs to pass laws which give the government the power to ensure the safety of not only its citizens but also the medical professionals and institutions.

References

1. Alon, S., & Shoham, S. (2024). The role of responsibility in AI-assisted medicine: Legal and ethical implications. Journal of Law, Medicine & Ethics, 52(2), 408–423.
2. Baker, S., & Xiang, W. (2023). Explainable AI is Responsible AI: How Explainability Creates Trustworthy and Socially Responsible Artificial Intelligence. ArXiv. https://arxiv.org/abs/2312.01555
3. Bharati, R. (2024). Artificial intelligence: Legal and regulatory challenges in India. YMER Digital. https://ymerdigital.com/uploads/YMER230787.pdf
4. Bharati, R. (2024). Regulation of artificial intelligence in India: Difficulties and factors to be considered. ResearchGate. https://www.researchgate.net/publication/384546715_Regulation_of_Artificial_Intelligence_in_India_Difficulties_and_Factors_to_be_Considered
5. Bhattacharya, S., Singh, A., & Hossain, M. (2020). Digital health governance in India: Policy and regulatory perspectives. Health Policy and Technology, 9(4), 100–110.
6. Brey, P. (2012). Anticipatory ethics for emerging technologies. NanoEthics, 6(1), 1–13.
7. Centre for Internet and Society. (n.d.). AI in India: A policy agenda. https://cis-india.org/internetgovernance/files/ai-in-india-a-policy-agenda
8. Chatterjee, P. (2015). India plans National eHealth Authority. The Lancet, 386(10011), 2245–2246.
9. Chatterjee, S. and Dohan, M. S. (2021). Artificial Intelligence for Healthcare in India. International Journal of Healthcare Information Systems and Informatics, 16(4), 1-11. https://doi.org/10.4018/ijhisi.20211001.oa17
10. Chaudhuri, S., et al. (2020b). Legal and regulatory framework for e-health in India. Journal of Health Management, 22(3), 1–12.
11. Digital Personal Data Protection Act, 2023 (India).
12. Esteva, A., Kuprel, B., Novoa, R., Ko, J., Swetter, S., Blau, H., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118.

13.European Parliament & Council of the European Union. (2024). Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
14.Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1).
15.Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
16.Food and Drug Administration. (2021). Artificial intelligence/machine learning (AI/ML)-based software as a medical device action plan. U.S. Department of Health and Human Services.
17.Fredrick, O. (2025, May 21). 5 real-world examples of failed AI projects in developing countries and their lessons. Medium. https://medium.com/@otimfredrick/5-real-worldexamples-of-failed-ai-projects-in-developing-countries-and-their-lessons-9b74f122721c
18.Government of India. (2023). The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice.
19.Greenleaf, G. (2023). India's Digital Personal Data Protection Act 2023: Implications for global data governance. Privacy Laws & Business International Report, 185, 1–5.
20.Indian Council of Medical Research. (2023). Ethical guidelines for application of artificial intelligence in biomedical research and healthcare. New Delhi: ICMR.
21.Information Technology Act, 2000 (India Code updated 2023). (2023). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
22.Jain, D. (2023). Regulation of digital healthcare in India: Ethical and legal concerns. Digital Health, 12. https://pmc.ncbi.nlm.nih.gov/articles/PMC10048681
23.Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
24.Mak, K. K., & Pichika, M. R. (2019). Artificial intelligence in drug development: Present status and prospects. Drug Discovery Today, 24(3), 773–780.
25.Mark, B., & Bizz, P. (2025). Ethical Implications of AI-Driven Decision Making in Healthcare Information Systems. Preprints. https://doi.org/10.20944/preprints202503.0078.v1
26.Medical Council of India v. Dr. Yash Pal Ghai (2007). Supreme Court of India verdict (illustrative of traditional negligence principles derived from Indian jurisprudence; see Murthy, 2007 for context).
27.Medical Device Rules, 2017 (India).
28.Ministry of Electronics & Information Technology. (2024). Report on artificial intelligence. Government of India. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
29.Ministry of Electronics & Information Technology. (2025). India AI governance guidelines. Government of India.
30.Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act. Government of India.
31.Ministry of Health & Family Welfare. (2026). Strategy for artificial intelligence in healthcare for India (SAHI). Government of India.
32.Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501–507.
33.Mooghali, M., Stroud, A. M., Yoo, D. W., Barry, B. A., Grimshaw, A. A., Ross, J. S., & Miller, J. E. (2024). Trustworthy and ethical AI-enabled healthcare: A rapid review. BMC Medical Informatics and Decision Making, 24, 247.
34.Murphy, K., Di Ruggiero, E., Upshur, R. et al. Artificial intelligence for good health: a scoping review of the ethics literature. BMC Med Ethics 22, 14 (2021). https://doi.org/10.1186/s12910-021-00577-8
35.Murthy, K. S. (2007). Medical negligence in India: Contemporary perspectives. Indian Journal of Medical Ethics, 4(2), 60–65.
36.National Health Authority. (2022). Health data management policy under Ayushman Bharat Digital Mission. Government of India.
37.National Health Authority. (2022). Health data management policy under Ayushman Bharat Digital Mission. Government of India.
38.National Medical Commission. (2002). Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
39.Nishith Desai Associates. (2025). Artificial intelligence in healthcare—Navigating regulatory frontiers in India. https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Artificial-Intelligencein-Healthcare.pdf
40.Nishith Desai Associates. Artificial Intelligence in Healthcare: Navigating Regulatory Frontiers in India. March 2025. © Nishith Desai Associates 2025. Available at: www.nishithdesai.com. DMS Code: 119795.2.
41.NITI Aayog. (2018). National strategy for artificial intelligence. Government of India.
42.NITI Aayog. (2021). Responsible AI for All: Approach document for India. Government of India.

43.NITI Aayog. (2021). Towards responsible #AIforAll: Approach document for India – Part 1. Government of India. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
44.NITI Aayog. (2023). National strategy for artificial intelligence. Government of India. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
45.Nowakowski, W. (2022). Ethical and social implications of artificial intelligence in healthcare. Journal of Humanities and Applied Science Research, 5(1), 111–120.
46.Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the future — Big data, machine learning and clinical medicine. New England Journal of Medicine, 375(13), 1216–1219.
47.Paul, M. (2009). Privacy concerns in anonymized datasets: Risks of re-identification. Information Security Journal, 18(5), 215–222.
48.Povie, G. (2021). Medical AI: Legal accountability and risk management frameworks. Artificial Intelligence and Law, 29(3), 375–400.
49.Pradhan, K., John, P., & Sandhu, N. (2021). Use of artificial intelligence in healthcare delivery in India. Journal of Hospital Management & Health Policy, 5. https://jhmhp.amegroups.org/article/view/6765/html
50.Prakash, R. V., Reddy, G. S., & Balle, S. (2025). Ethical considerations in artificial intelligence for healthcare: Addressing bias, privacy and accountability. International Journal of Healthcare Technology.
51.Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. New England Journal of Medicine, 380(14), 1347–1358.
52.Santosh Kumar, & Agarwal, R. (n.d.). AI-driven telemedicine in India: Challenges and opportunities. Telehealth and Medicine Today. https://telehealthandmedicinetoday.com/index.php/journal/article/download/252/388/1925
53.Sharma, A. (2024). The legal implications of artificial intelligence and machine learning in Indian healthcare. ResearchGate.
https://www.researchgate.net/publication/381009921_The_Legal_Implications_of_Artificial_Intelligence_and_Machine_Learning_in_Indian_Healthcare
54.Sheikh, M. (2020). Artificial intelligence and legal policy: A review. Asian Pacific Law & Policy Review. https://thelawbrigade.com/wp-content/uploads/2020/09/Sheikh-Mahwesh-APLPR.pdf
55.Sreenivasulu, N., et al. (2019). Electronic health records and privacy challenges in India. Indian Journal of Medical Ethics, 4(2), 95–102.
56.Surden, H. (2020). Artificial intelligence and legal liability. Vanderbilt Law Review, 73(4), 1305–1354.
57.Telecommunication Engineering Centre. (2020). AI policies in India: A status paper. Government of India. https://www.tec.gov.in/pdf/Studypaper/AI%20Policies%20in%20India%20A%20status%20Paper%20final
58.The Digital Personal Data Protection Act, 2023 (India Code). (2023). https://www.indiacode.nic.in/handle/123456789/20062
59.Topol, E. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56.
60.Topol, E. (2019). High-performance medicine: The convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56.
61.Vayena, E., Blasimme, A., & Cohen, I. G. (2018). Machine learning in medicine: Addressing ethical challenges. PLoS Medicine, 15(11).
62.Weiner, E. B., Dankwa-Mullan, I., Nelson, W. A., & Hassanpour, S. (2024). Ethical Challenges and Evolving Strategies in the Integration of Artificial Intelligence into Clinical Practice. ArXiv. https://arxiv.org/abs/2412.03576
63.Weiner, E. B., Dankwa-Mullan, I., Nelson, W. A., & Hassanpour, S. (2024). Ethical challenges in the integration of artificial intelligence into healthcare. Journal of Medical Ethics.
64.World Health Organization. (2021). Ethics and governance of artificial intelligence for health. Geneva: WHO.
65.Zhang, B., & Dafoe, A. (2019). Artificial intelligence: American attitudes and trends. AI & Society, 34(1), 1–18.