Transformative Digital Practices for Social Equity: A Study of AI Adoption in Healthcare Through the Ayushman Bharat Digital Mission for a Future-Ready Society

Seema B[1], Vidya A. R[2]

[1]Assistant Professor, Christ Academy Institute of Law, Bengaluru

[2]Associate Professor, Alva's Law College, Moodabidre

DOI: https://doi.org/10.51244/IJRSI.2026.1315PH00209

Received: 05 November 2026; Accepted: 10 November 2026; Published: 25 November 2026

ABSTRACT

Artificial intelligence (AI) is increasingly being used to support medical diagnosis, clinical decision-making, patient monitoring and the management of healthcare services. In India, the potential of these technologies must be considered alongside the Ayushman Bharat Digital Mission (ABDM), which seeks to create an interoperable digital health ecosystem. This paper examines whether the adoption of AI can contribute to social equity in healthcare and what institutional, managerial and legal conditions are necessary for that contribution to be realised. It combines a review of selected academic and policy literature, an examination of the Indian legal framework and a small exploratory questionnaire study involving 19 medical professionals working in different healthcare settings. The survey findings indicate that respondents generally perceived some improvement in work efficiency, while also identifying patient data privacy, algorithmic bias, accountability, limited skills, technical support, and system integration as important concerns. The small sample does not permit national generalisation; rather, it provides an exploratory account of professional experience. The paper argues that ABDM should be understood as digital public infrastructure that may enable responsible data use, not as proof that AI has been uniformly adopted across the health system. It concludes that AI-enabled healthcare can advance social equity only when digital infrastructure is accompanied by clinical validation, human oversight, workforce development, inclusive access, privacy safeguards and clear accountability. The analysis is situated within the constitutional guarantees of equality, dignity, and privacy; the Digital Personal Data Protection Act, 2023 and its phased commencement; applicable medical-device regulation; and relevant international guidance.

Keywords: Artificial Intelligence; Healthcare; Ayushman Bharat Digital Mission; Social Equity; Digital Health; Data Protection; Patient Rights; Viksit Bharat 2047.

1. INTRODUCTION

Access to healthcare is not determined solely by the availability of medical knowledge. It is also shaped by geography, income, institutional capacity, the availability of trained professionals and the ability of individuals to obtain timely and appropriate treatment. These barriers are particularly important in a country as diverse as India, where healthcare resources and digital infrastructure are not evenly distributed. A technology that improves diagnosis in a well-equipped urban hospital may have a very different impact in a rural primary health centre with limited connectivity, equipment or specialist support.

Artificial intelligence has the potential to assist healthcare professionals in interpreting medical images, identifying patterns in clinical data, supporting risk assessment, monitoring patients and reducing certain administrative tasks. Bajwa et al. (2021) explain that AI may transform medical practice, but emphasise the need to build reliable, safe systems. The World Health Organisation (WHO, 2021) similarly cautions that AI in health must be developed and used with human rights and ethical considerations at its centre. These perspectives suggest that the value of AI cannot be measured only by speed, automation or cost reduction. Its value must also be assessed by its effect on patient welfare, safety, dignity and access.

In India, the Ayushman Bharat Digital Mission provides an important institutional context for this discussion. ABDM aims to develop the digital infrastructure required to connect individuals, healthcare professionals and health facilities through a digital health ecosystem. Its components include the Ayushman Bharat Health Account (ABHA), the Healthcare Professionals Registry and the Health Facility Registry. Such infrastructure may support the availability and exchange of health information, subject to appropriate consent, security and governance arrangements. However, the existence of a digital health infrastructure should not be confused with the widespread deployment of AI tools within ABDM or across all healthcare institutions. The distinction between digitalisation and AI adoption is central to this paper.

The paper therefore examines AI adoption as a combined question of technology, management and law. It considers whether healthcare institutions have the skills and organisational capacity to use AI; whether AI can help reduce disparities in access; and whether the existing legal framework adequately protects patients when algorithmic systems influence healthcare decisions. The larger policy context is the vision of Viksit Bharat 2047, which requires development to be inclusive and responsive to the needs of all sections of society.

2. RESEARCH PROBLEM AND OBJECTIVES

The central research problem is the gap between the promise of AI-enabled healthcare and the conditions required for its safe, equitable and accountable use in India. Digital tools may improve service delivery, but they may also reproduce existing inequalities where access to devices, connectivity, quality data and trained personnel is uneven. In addition, AI-assisted decisions can raise questions about privacy, informed consent, clinical responsibility and remedies when harm occurs.

1. To identify selected AI applications used in private and other healthcare settings, as reported in the study material and by respondents.

2. To examine the role of ABDM as digital health infrastructure and its potential relationship with AI-enabled healthcare.

3. To identify perceived benefits, institutional barriers and ethical concerns associated with AI adoption among the medical professionals surveyed.

4. To analyse the constitutional, statutory and policy framework relevant to AI-enabled healthcare in India.

5. To suggest legal, institutional and managerial measures that can support safe, inclusive and accountable AI adoption.

3. RESEARCH QUESTIONS

6. How do healthcare professionals participating in the exploratory survey perceive the use and impact of AI in their work?

7. What institutional and managerial conditions influence the adoption of AI in healthcare?

8. How can ABDM support the digital foundations for AI-enabled healthcare without compromising patient rights?

9. To what extent do India's existing constitutional and statutory frameworks address privacy, safety and accountability concerns arising from AI-assisted healthcare?

4. REVIEW OF LITERATURE AND POLICY CONTEXT

4.1 AI and the changing practice of medicine

Bajwa et al. (2021) describe the potential of AI to strengthen diagnosis, clinical decision support and the delivery of healthcare. Their analysis is useful because it treats implementation as more than the installation of

software. Reliable data, clinical validation, appropriate infrastructure, and continuous monitoring are necessary for AI systems to support rather than undermine medical practice. This is particularly relevant to India, where the capacity to adopt new technologies varies across institutions and regions.

Akila et al. (2025) discuss applications of AI in areas such as medical imaging, personalised treatment, predictive healthcare and hospital administration. They also identify concerns involving privacy, bias, transparency and regulatory uncertainty. Their review reinforces the need to consider the conditions under which AI is used, rather than assuming that technological availability will automatically produce better health outcomes.

4.2 Adoption, professional readiness and organisational capacity

Adoption is distinct from technological development. A tool may exist and may have been tested, yet remain unused in routine clinical practice. Nguyen et al. (2025), using data from the United States Business Trends and Outlook Survey, found that AI use among healthcare firms averaged 5.9 per cent over the study period and reached 8.3 per cent in 2025. They also found variation between healthcare subsectors. These findings cannot be transferred directly to India, but they illustrate why claims about adoption should be based on evidence of actual use rather than on the number of available products or policy announcements.

An Indian cross-sectional survey by Raj et al. (2025), involving 572 healthcare professionals, reported gaps in technical knowledge and expertise, as well as interest in the future use of AI. The study is relevant to the present research because it places professional readiness at the centre of implementation. AI literacy, continuing training, and the ability to evaluate an algorithm's limitations are important for ensuring that clinical professionals retain meaningful control over patient care.

4.3 Global policy guidance

The WHO's guidance on ethics and governance of AI for health identifies six principles intended to ensure that AI serves the public interest. These include protecting human autonomy; promoting human well-being and safety; ensuring transparency and explainability; fostering responsibility and accountability; ensuring inclusiveness and equity; and promoting responsive and sustainable AI. The guidance provides a rights-oriented framework that is relevant to countries at different stages of digital health development (WHO, 2021).

The World Economic Forum and Boston Consulting Group (2025) identify the need for stronger governance, digital infrastructure, collaboration and trust if AI-enabled healthcare is to be implemented at scale. The European Commission's policy material provides a comparative regulatory perspective: AI systems intended for medical purposes may fall within high-risk regulatory requirements under the EU AI Act, including risk management, data quality, user information and human oversight. These frameworks are not binding in India, but they offer useful reference points for policy design.

4.4 Research gap

The literature reviewed addresses AI's clinical potential, adoption barriers, professional readiness and global governance principles. However, these themes need to be brought together in the Indian context. In particular, there is a need to examine how digital health infrastructure, institutional capacity, patient data protection and clinical accountability interact. The present paper contributes an exploratory professional survey and a legal analysis to this discussion. Given the limited sample size, it does not claim to provide a nationally representative measure of AI adoption.

5. RESEARCH METHODOLOGY

Research Design

The study adopts an exploratory, interdisciplinary design that combines a review of selected academic and policy literature, doctrinal legal analysis, and a structured questionnaire administered to medical professionals. The 19 respondents were drawn from private hospitals, government hospitals, a clinic and other healthcare

settings. The original research notes describe the sampling approach as random sampling. The quantitative responses are presented descriptively, using the counts and percentages from the original tables. The survey is treated as exploratory. ABDM is best understood as a digital public infrastructure initiative intended to facilitate the creation and exchange of digital health information across participating individuals, professionals and facilities. The ABHA number provides an identifier within the digital health ecosystem, while the registries are intended to improve the discoverability of verified professionals and health facilities. These components may support continuity of care and the availability of data for legitimate healthcare purposes. They do not, by themselves, establish that a particular AI application has been adopted, clinically validated or deployed at scale.

AI applications discussed in the source material include image-based screening and diagnostic support, clinical decision support systems, electronic health records, predictive analytics, chatbots, remote monitoring, and robotic-assisted procedures. Examples named in the material include qXR/Qure.ai-related chest imaging applications, AI-assisted retinal screening, fetal and neonatal monitoring technologies, and AI-enabled clinical support tools. The paper does not treat every named product as an ABDM-owned or ABDM-deployed system. Their regulatory status, current deployment, validation evidence and institutional use should be independently documented before any product-specific claim is made.

ABDM may create conditions that support AI research and implementation by enabling interoperable digital records and a more connected health information environment. That potential depends on data quality, representativeness, security, lawful access and governance. Data that systematically under-represents rural populations, women, older persons, persons with disabilities or particular disease groups may produce systems that perform less reliably for those communities. Interoperability must therefore be accompanied by standards for data quality and safeguards against inappropriate access or secondary use.

6. EMPIRICAL FINDINGS

The questionnaire responses provide a limited but useful picture of how participating professionals experience AI and related digital systems. The tables below reproduce the figures in the supplied research material. Percentages are retained as reported.

6.1 Perceived effect on work efficiency

Among the 11 respondents from private hospitals, 8 (72.7 per cent) reported that AI had somewhat improved work efficiency and 2 (18.2 per cent) reported significant improvement. One respondent (9.1 per cent) reported no change. Among six respondents from government hospitals, four (66.7 per cent) reported some improvement, one (16.7 per cent) reported significant improvement, and one (16.7 per cent) reported no change. The single clinic respondent reported some improvement. One respondent categorised as 'Other' did not provide a response.

Table 1. Type of healthcare setting and perceived effect of AI on work efficiency (n = 19)

Type of hospital	Somewhat improved	Significantly improved	No change	No response	Total
Private (n=11)	8 (72.7%)	2 (18.2%)	1 (9.1%)	0	11
Government (n=6)	4 (66.7%)	1 (16.7%)	1 (16.7%)	0	6
Clinic (n=1)	1 (100%)	0	0	0	1
Other (n=1)	0	0	0	1 (100%)	1
Total (n=19)	13	3	2	1	19

6.2 AI tools and reported uses

The responses refer to AI chatbots or virtual assistants, electronic health records, clinical decision-support systems, diagnostic imaging applications, pathology or laboratory analysis and predictive analytics. The most

frequently reported category among clinical-speciality respondents was AI chatbots or virtual assistants (4; 21.1 per cent), followed by electronic health records (3; 15.8 per cent). Diagnostic imaging AI, AI chatbots in diagnostic and imaging fields, and other categories were reported by smaller numbers. The table indicates that respondents described a mixture of clinical, administrative and research-related uses. It does not establish the accuracy or clinical effectiveness of the tools.

Table 2. AI tools and primary uses reported by respondents (n = 19)

Reported tool/use category	Frequency	Percentage	Illustrative purpose reported
AI chatbots/virtual assistants (clinical specialities)	4	21.10%	Diagnosis, administration or research
Electronic health records (clinical specialities)	3	15.80%	Administrative tasks
Clinical decision-support systems	1	5.30%	Monitoring or research
Diagnostic imaging AI	2	10.50%	Diagnosis and treatment
AI chatbots (diagnostic/imaging fields)	2	10.50%	Research or diagnosis
AI in pathology/laboratory analysis	1	5.30%	Diagnosis or administration
Electronic health records (emergency/critical care)	1	5.30%	Diagnosis, monitoring or administration
Administrative use; no tool specified	1	5.30%	Administrative tasks
Clinical decision support (obstetrics and gynaecology)	1	5.30%	Research
Surgical specialities; no tool specified	1	5.30%	Not specified
Electronic health records (other)	1	5.30%	Monitoring or administration
Predictive analytics (other)	1	5.30%	Research
Total	19	100%	

6.3 Ethical concerns and barriers

Patient data privacy was identified as an individual ethical concern by four respondents (21.1 per cent); algorithmic bias and accountability were each identified by three respondents (15.8 per cent). Eight respondents (42.1 per cent) selected or reported multiple ethical concerns. On implementation barriers, lack of skills or training and multiple barriers were each reported by four respondents (21.1 per cent). Technical support issues and integration with existing systems were each reported by three respondents (15.8 per cent), while two respondents (10.5 per cent) identified legal or regulatory issues. Three respondents did not answer the barriers question.

Table 3. Ethical concerns and barriers to AI adoption (n = 19)

Category	Issue	Frequency	Percentage
Ethical concern	Patient-data privacy	4	21.10%
Ethical concern	Algorithmic bias	3	15.80%
Ethical concern	Accountability	3	15.80%
Ethical concern	Multiple ethical concerns	8	42.10%
Ethical concern	No response	1	5.30%
Barrier	Lack of skills/training	4	21.10%
Barrier	Technical support	3	15.80%
Barrier	Integration with existing systems	3	15.80%
Barrier	Legal/regulatory issues	2	10.50%
Barrier	Multiple barriers	4	21.10%
Barrier	No response	3	15.80%

6.4 Interpretation of the findings

The responses suggest that participants see practical value in AI and related digital tools, particularly in improving work processes. At the same time, they identify concerns that go to the heart of responsible implementation: privacy, bias, accountability, training, and technical integration. These are not peripheral matters. A system that is efficient but poorly validated, insecure, or difficult for clinicians to interpret may expose patients to harm and weaken trust in healthcare institutions.

7. LEGAL AND CONSTITUTIONAL FRAMEWORK IN INDIA

7.1 Equality, non-discrimination and access

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws. In the context of AI-enabled healthcare, the constitutional concern is not that every algorithmic difference necessarily amounts to discrimination. Rather, the concern is whether a public authority or healthcare system uses a tool in a manner that results in arbitrary or unjustifiably unequal access, treatment, or outcomes. If training data fail to represent particular communities, or if a system performs less accurately for them, the resulting disparities may require legal and institutional scrutiny. The principle of non-arbitrariness associated with Article 14 therefore supports requirements for validation, monitoring and review.

Social equity also requires attention to the digital divide. AI-enabled services should not become available only to patients who have smartphones, reliable connectivity, digital literacy or the ability to pay. Public healthcare institutions must maintain accessible non-digital pathways and provide appropriate assistance to people who cannot use digital systems independently. AI should supplement the health system's capacity, not become a condition for obtaining essential care.

7.2 Right to life, health and dignity

Article 21 protects life and personal liberty. In Paschim Banga Khet Mazdoor Samity v. State of West Bengal (1996), the Supreme Court recognised the State's obligation to preserve human life by providing timely medical treatment. The decision provides an important constitutional foundation for examining the State's responsibility in healthcare delivery. AI may support that responsibility when it improves timely diagnosis or resource allocation; it may undermine it if unvalidated systems delay treatment, produce unsafe recommendations or exclude vulnerable patients.

Human dignity and autonomy must remain central to clinical decision-making. AI systems should assist qualified professionals rather than displace clinical responsibility. Patients should be given understandable information when AI materially contributes to a diagnosis, risk assessment or treatment recommendation, particularly where that information affects consent or the patient's ability to question a decision.

7.3 Privacy and protection of health information

In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge bench recognised privacy as a constitutionally protected right connected with liberty, dignity and autonomy. Health information can reveal intimate details about an individual's body, family history, mental health and personal circumstances. Its collection and use therefore require a clear legal basis and safeguards proportionate to the purpose. The judgment's proportionality framework is relevant when state action or public digital health systems process personal information.

The Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a statutory framework for the processing of digital personal data. Its provisions address matters including notice, consent, legitimate uses, obligations of data fiduciaries, security safeguards and the rights of individuals. The Act does not create a separate category of 'sensitive personal data' in the same manner as the earlier draft framework; nevertheless, health information is personal data and its processing can carry serious consequences for individuals. The Act's commencement must be stated accurately: by notification G.S.R. 843(E) dated 13 November 2025, different provisions were brought into force on different dates. The core processing obligations in sections 3–17 were

scheduled to commence 18 months after publication, i.e. 13 May 2027. Accordingly, as at 13 November 2026, those core obligations had not yet commenced. The DPDP Rules, 2025 were notified by G.S.R. 846(E) on 13 November 2025, with their own phased commencement arrangements.

Until the relevant DPDP provisions come into force, the legal position must also be considered with reference to the Information Technology Act, 2000, and the rules and directions applicable at the time. Section 43A of the IT Act and the Sensitive Personal Data or Information Rules, 2011 have historically been relevant to the handling of sensitive personal data by body corporates; Section 72A addresses disclosure of information in breach of lawful contract. The statutory position is subject to the DPDP Act's amendment and commencement scheme. It would therefore be inaccurate to state simply that the DPDP Act's entire substantive regime is already fully operational.

7.4 Consent, patient autonomy and clinical responsibility

In Samira Kohli v. Dr Prabha Manchanda (2008), the Supreme Court explained the requirements of valid informed consent in medical treatment. In AI-enabled care, consent is not meaningful merely because a patient clicks an acceptance box. Patients should, where relevant, understand the role of AI in their care, the purpose of its use of their information, the system's limits, and whether their data may be used for research or model development. The information should be communicated in a manner that is understandable to the patient and appropriate to the clinical context.

7.5 Medical-device regulation and professional standards

India does not currently regulate every aspect of AI in healthcare through a single dedicated AI-health statute. However, it would be too broad to conclude that AI medical software is wholly unregulated. The Central Drugs Standard Control Organisation states that medical devices in India are regulated under the Drugs and Cosmetics Act, 1940 and the Medical Devices Rules, 2017; the definition of medical device includes software intended for specified medical purposes. Whether a particular AI application is regulated as a medical device depends on its intended purpose and classification. This makes product-specific regulatory assessment important.

The National Medical Commission Act, 2019, and the applicable professional conduct requirements remain relevant to medical practitioners. AI assistance does not remove the practitioner's obligation to exercise professional judgment. In Jacob Mathew v. State of Punjab (2005), the Supreme Court discussed the standard applicable to medical negligence. In an AI-assisted setting, the question may include whether a practitioner reasonably evaluated the system's output, considered the patient's clinical circumstances and acted consistently with accepted professional standards. The precise standard will depend on the facts and available evidence.

7.6 Liability of hospitals, developers and service providers

Responsibility for harm may extend beyond the treating practitioner. A hospital may be responsible for decisions about procurement, validation, staff training, system configuration, supervision and incident response. Developers and suppliers may bear responsibility where defects, inadequate warnings, misleading performance claims or failures in design and maintenance cause harm. The Consumer Protection Act, 2019 contains a product-liability framework, including provisions dealing with manufacturers, product service providers and product sellers. Whether a particular AI product or service falls within the statutory definitions and whether the required elements of a claim are established must be determined on the facts; liability should not be assumed merely because an AI system was involved.

8. INTERNATIONAL AND COMPARATIVE PERSPECTIVES

The WHO guidance offers a useful normative baseline for India because it links AI governance with autonomy, safety, transparency, accountability, inclusiveness and sustainability. Its approach supports a model in which AI systems are assessed throughout their lifecycle, from design and validation to deployment,

monitoring and retirement. It also emphasises that the benefits of AI should be shared across countries and communities rather than concentrated in settings with greater technological resources.

The European Union provides a more formal regulatory comparator. Under Regulation (EU) 2024/1689, the AI Act, certain AI systems used as safety components of products or as products covered by specified harmonisation legislation may be classified as high-risk. The European Commission identifies AI-based software intended for medical purposes as an area where high-risk requirements may apply. These requirements include risk management, data governance, technical documentation, transparency and human oversight, subject to the Act's scope and transitional timetable. The EU framework is not directly applicable in India, but it demonstrates how AI-specific obligations can be integrated with existing medical-device regulation.

The comparative lesson is not that India should copy another jurisdiction wholesale. India's regulatory approach must account for its public health system, federal structure, resource constraints and the role of digital public infrastructure. Nevertheless, risk-based classification, lifecycle monitoring, independent evaluation, clear allocation of responsibility and effective remedies are relevant principles for domestic reform.

9. DISCUSSION: CONNECTING TECHNOLOGY, MANAGEMENT AND SOCIAL EQUITY

The empirical findings and the literature point towards a common conclusion: AI adoption is an organisational process, not simply a technological purchase. Hospitals require clear leadership, procurement standards, reliable infrastructure, staff training, interoperability and procedures for reviewing system performance. Management must also decide who is responsible for monitoring outputs, responding to errors, documenting human overrides and reporting adverse events. Without these arrangements, even a technically capable system may be poorly integrated into clinical practice.

First, AI literacy should be treated as a continuing professional-development requirement. Doctors, nurses, technicians and administrators need role-specific training that explains what a system can and cannot do, how its performance is measured and when its output should be questioned. The survey's identification of skills and training as a recurring barrier supports this priority, although the small sample means the finding should be interpreted as indicative rather than representative.

Second, hospitals and public health authorities should use a structured procurement and validation process. Before deployment, an AI tool should be assessed for its intended use, clinical evidence, accuracy across relevant population groups, cybersecurity, interoperability, usability and regulatory status. After deployment, performance should be monitored in real-world conditions. A tool that performs well in one institution or population may not perform equally well elsewhere.

Third, data governance must be built into the design of digital health programmes. Access should be purpose-specific and role-based; data should be protected against unauthorised access; and secondary use for research or commercial model development should be governed by a clear legal and ethical framework. Consent mechanisms should be meaningful and accessible, and patients should have channels to raise concerns or seek correction where appropriate.

Fourth, social equity should be an explicit performance measure. Public authorities should assess whether AI-enabled services reach rural communities, low-income groups, older persons, persons with disabilities and people with limited digital literacy. Language accessibility, affordability, connectivity and the availability of human assistance are not optional additions; they influence whether a digital health intervention is genuinely accessible.

Finally, accountability should be shared but clearly allocated. Medical professionals remain responsible for professional judgment; hospitals are responsible for institutional deployment and oversight; developers and suppliers are responsible for the quality and safety obligations applicable to their products and services; and public authorities are responsible for appropriate regulation and system-level governance. Clear documentation

and accessible grievance mechanisms are necessary to prevent responsibility from disappearing between these actors.

10. RECOMMENDATIONS

Adopt a risk-based governance framework for AI-enabled healthcare, distinguishing administrative tools from systems that materially influence diagnosis, triage or treatment.

Require documented clinical validation, population-relevant testing, cybersecurity assessment and periodic performance audits before and after deployment.

Develop practical AI-literacy programmes for doctors, nurses, allied health professionals, administrators and public health personnel.

Clarify institutional responsibilities through written policies covering procurement, human oversight, incident reporting, system updates, record-keeping, and patient communication.

Strengthen ABDM data governance by ensuring purpose limitation, secure access, interoperability standards, data quality and meaningful safeguards for secondary use.

Maintain accessible alternatives and human assistance so that patients are not excluded due to limited connectivity, devices, literacy, language, or ability to pay.

Provide clear information to patients when AI materially contributes to a clinical decision, and preserve meaningful opportunities for human review and clinical escalation.

Review the interaction between medical-device regulation, professional standards, consumer protection and data-protection law to reduce gaps and uncertainty in accountability.

Support independent research using representative Indian datasets and transparent evaluation methods, with appropriate ethics review and privacy safeguards.

Publish periodic, disaggregated information on AI adoption and outcomes in public and private healthcare settings, while protecting confidential and personal data.

11. LIMITATIONS AND FUTURE RESEARCH

This study is limited by the small sample of 19 respondents and the absence of information in the supplied material on survey dates, location, sampling frame, questionnaire validation, and response rate. The results are descriptive and should not be generalised to the Indian healthcare sector as a whole. The table concerning perceived accuracy and patient safety contains an internal inconsistency and requires verification against the original responses. The paper also does not independently audit the clinical performance or regulatory status of each AI product named in the source material.

Future research may use a larger, geographically diverse sample and compare public and private institutions, urban and rural facilities, and different clinical specialities. Further work may examine the actual use of AI within ABDM-linked institutions, the quality and representativeness of health datasets, patient awareness of AI-assisted care, and the allocation of liability when algorithmic outputs contribute to adverse outcomes. A comparative study of India's framework with the EU AI Act and other risk-based governance models may also assist in developing context-sensitive regulatory proposals.

12. CONCLUSION

AI has the potential to improve healthcare delivery in India, but its contribution to social equity cannot be assumed from technological progress alone. The exploratory responses in this study indicate perceived improvements in work efficiency while drawing attention to privacy, bias, accountability, training and

technical integration. The literature and international guidance similarly show that safe adoption depends on reliable evidence, institutional readiness, and meaningful human oversight.

ABDM can provide important digital foundations for a more connected health system. Its role should, however, be accurately described: digital health infrastructure can enable the responsible use of data, but it does not, by itself, demonstrate widespread AI adoption or guarantee equitable outcomes. Those outcomes depend on how institutions govern data, select and validate tools, train professionals and ensure that patients can access services without discrimination.

India's constitutional commitments to equality, life, dignity and privacy provide the normative foundation for this approach. Existing laws and regulatory mechanisms address several relevant dimensions, but the interaction among AI systems, medical device regulation, professional duties, data protection, and product liability requires continued attention. A coherent governance framework should encourage innovation while making safety, fairness and accountability enforceable in practice. Ultimately, the success of AI in Indian healthcare should be measured not by the number of systems introduced, but by whether they deliver safe, affordable and accessible care while protecting the rights and dignity of every patient.

REFERENCES

1. Akila, K., Gopinathan, R., Arunkumar, J., & Malar, B. S. B. (2025). The role of artificial intelligence in modern healthcare: Advances, challenges, and future prospects. European Journal of Cardiovascular Medicine, 15(4), 615–624. https://doi.org/10.61336/ejcm/25-04-94
2. Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: Transforming the practice of medicine. Future Healthcare Journal, 8(2), e188–e194. https://doi.org/10.7861/fhj.2021-0095
3. Central Drugs Standard Control Organisation. (n.d.). Medical devices and diagnostics. Government of India. https://www.cdsco.gov.in/opencms/opencms/en/Medical-Device-Diagnostics/Medical-Device-Diagnostics/
4. European Commission. (n.d.). Artificial intelligence in healthcare. Directorate-General for Health and Food Safety. https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en
5. Government of India. (2000). Information Technology Act, 2000.
6. Government of India. (2017). Medical Devices Rules, 2017.
7. Government of India. (2019). National Medical Commission Act, 2019.
8. Government of India. (2019). Consumer Protection Act, 2019.
9. Government of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf
10. Government of India, Ministry of Electronics and Information Technology. (2025, November 13). Notification G.S.R. 843(E): Commencement of provisions of the Digital Personal Data Protection Act, 2023.
11. Government of India, Ministry of Electronics and Information Technology. (2025, November 13). Notification G.S.R. 846(E): Digital Personal Data Protection Rules, 2025.
12. Indian Council of Medical Research. (2023). Ethical guidelines for application of artificial intelligence in biomedical research and healthcare. https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare
13. Jiang, L., Wu, Z., Xu, X., Zhan, Y., Jin, X., Wang, L., & Qiu, Y. (2021). Opportunities and challenges of artificial intelligence in the medical field: Current application, emerging problems, and problem-solving strategies. *Journal of International Medical Research, 49*(3), 1–11. https://doi.org/10.1177/03000605211000157
14. Nguyen, T. D., Whaley, C. M., Simon, K., Mehta, N., Yu, H., McBain, R. K., Mehrotra, A., & Cantor, J. H. (2025). Adoption of artificial intelligence in the health care sector. JAMA Health Forum, 6(11), e255029. https://doi.org/10.1001/jamahealthforum.2025.5029
15. Raj, P., Singh, A., Singh, K., & Datta, R. (2025). Adoption of artificial intelligence technologies in health care: A cross-sectional survey on insights and perspectives of healthcare professionals. *Medical Journal Armed Forces India, 81*(6). https://doi.org/10.1016/j.mjafi.2025.04.012

16. World Economic Forum, in collaboration with Boston Consulting Group. (2025). The future of AI-enabled health: Leading the way. https://reports.weforum.org/docs/WEF_The_Future_of_AI_Enabled_Health_2025.pdf
17. World Health Organisation. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. https://www.who.int/publications/i/item/9789240029200
18. World Health Organisation. (n.d.). Harnessing artificial intelligence for health. https://www.who.int/teams/digital-health-and-innovation/harnessing-artificial-intelligence-for-health
19. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689). https://eur-lex.europa.eu/eli/reg/2024/1689/oj
20. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
21. Jacob Mathew v. State of Punjab, (2005) 6 SCC 1.
22. Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37.
23. Samira Kohli v. Dr Prabha Manchanda, (2008) 2 SCC 1.