Page 2321 - 2333

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Liability Framework to Regulate Artificial Intelligence in Healthcare

ASHISH KUMAR KUREEL[*] AND PROF. (DR.) BRIJENDRA SINGH YADAV[**]

ABSTRACT

Artificial intelligence is beginning to play an important role in contemporary healthcare, where it is applied to diagnosis, clinical support, triage, imaging, remote monitoring, drug development and hospital management. A problem of liability arises because artificial intelligence produces outputs that can contribute to patient risk, yet the system itself cannot bear liability in the way a medical professional, a hospital or a manufacturer does. A review of the literature shows that no dedicated regime governs artificial intelligence liability in healthcare, and it brings out the associated questions of justice, bias, accountability, transparency and information security. This article analyses six areas: patient data confidentiality, patient consent, algorithmic bias and discrimination, misdiagnosis, accountability, and the reuse of previous patient records. It concludes that a workable framework must combine the principles of medical negligence law with data protection, consumer protection and sectoral safety requirements, together with governance mechanisms for artificial intelligence such as human oversight, audit logs, explainability and grievance redressal. The approach is qualitative and comparative, resting on a study of the literature and a content analysis of existing legal instruments, including the Digital Personal Data Protection Act, 2023, the Ayushman Bharat Digital Mission privacy framework, and the guidance of the World Health Organization on artificial intelligence in health. The findings indicate that the existing legal framework offers a partial answer to these questions but not an integrated one. Healthcare artificial intelligence should be treated as a high-risk setting governed by layered liability: the developer answers for design defects and bias, the deploying entity, ordinarily the hospital, answers for implementation and monitoring, and the medical professional answers for negligence where the use of artificial intelligence still involves human judgment.

Keywords: *artificial intelligence, healthcare, liability, medical negligence, data protection, algorithmic bias, informed consent, Digital Personal Data Protection Act, Ayushman Bharat Digital Mission, EU AI Act*

[*] Author is a Ph.D. Scholar at School of Legal Studies, Chandigarh University, Unnao, Uttar Pradesh, India.
[**] Author is a Professor and Director at School of Legal Studies, Chandigarh University, Unnao, Uttar Pradesh, India.

 [ISSN 2581-5369]

I. INTRODUCTION

Artificial intelligence no longer belongs only to the research laboratory or to ordinary automation tools. In healthcare it has become an active participant in decision-making: it manages imaging data, finds patterns in archives, generates risk forecasts and suggests courses of treatment. The literature describes artificial intelligence as a technology that imitates human intelligence through machine learning and deep learning, and comments on a rate of development that outpaces the legal mechanisms needed to control it.[1] That mismatch matters most in healthcare, where malfunction, algorithms trained on poor data, and inadequately tested models can affect diagnosis.[2]

The healthcare system is a distinctive setting because it brings together life and death, physical safety, confidential medical information and responsibility. A hospital that adopts a digital triage system, a virtual radiology assistant or a risk-prediction tool does not merely purchase software. It assumes duties of consent, data minimisation, safety, fairness, supervision of the system and record keeping.

The law must therefore answer a set of connected questions. Who is responsible when something goes wrong? How is patient information to be collected? How much explanation is owed to the patient? Can a decision influenced by artificial intelligence be challenged? And may information obtained from a patient in the past be used to train a model?[3]

This article approaches the problem as a critical analysis of liability regulation. It builds on Harsh Kumar's doctoral study at PANJAB UNIVERSITY of liability for artificial intelligence entities, which concludes that the existing regimes are fragmented and inadequate, and it carries that conclusion into the healthcare setting.[4] It also takes account of regulatory developments. The Digital Personal Data Protection Act, 2023 supplies a general regime for personal data, while the Health Data Management Policy and consent architecture of the AYUSHMAN BHARAT DIGITAL MISSION represent an attempt to build privacy and consent into digital health.[5] Internationally, the guidance of the WORLD HEALTH ORGANIZATION and the European Union's Artificial Intelligence Act show a movement towards risk-based governance of healthcare

[1] Alan M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433 (1950); Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353 (2016).

[2] James Shaw, Frank Rudzicz, Trevor Jamieson & Avi Goldfarb, *Artificial Intelligence and the Implementation Challenge*, 21 J. MED. INTERNET RSCH. e13659 (2019).

[3] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, ss. 5-6, 11-13, India Code (2023).

[4] HARSH KUMAR, LEGAL FRAMEWORK TO REGULATE LIABILITY OF ARTIFICIAL INTELLIGENCE ENTITIES: A STUDY (2025) (Ph.D. thesis, Panjab Univ., Dep't of Law), http://hdl.handle.net/10603/673853.

[5] NATIONAL HEALTH AUTHORITY, *Health Data Management Policy* (MINISTRY OF HEALTH & FAMILY WELFARE, Gov't of India, Dec. 2020). A revised draft was released for public consultation on 23 April 2022.

 [ISSN 2581-5369]

artificial intelligence.[6] Taken together, these instruments establish that healthcare artificial intelligence cannot be governed by any single rule.

II. Statement of the research problem

The principal obstacle is the absence of a coherent liability framework for artificial intelligence in medicine. The familiar principles of negligence, consumer liability, product liability and hospital liability were developed for human decision-makers or for conventional medical devices. Artificial intelligence systems learn from data, alter their outputs during operation, are partly opaque, and distribute responsibility among developers, data suppliers, operators, hospital staff and cloud service providers. Identifying a responsible party is correspondingly difficult.[7]

The difficulty is sharper where the harm is not a catastrophic error but a quiet clinical misstep. A system may misread an X-ray, miss a signal in a large dataset, recommend the wrong course of treatment, or draw on medical history in a way that defeats a patient's expectation of privacy. Harms of this kind are hard to classify legally. A patient may never learn that artificial intelligence was used at all. Even where the system only advises the clinician, heavy reliance on it makes the line between software error and medical malpractice difficult to draw.

The literature consistently identifies three gaps: the absence of a clear rule on liability for damage caused by artificial intelligence, the undefined legal status of artificial intelligence actors, and the need for transparency and accountability.[8] Placed in the healthcare setting, those concerns produce a practical regulatory vacuum in which patient rights exist in principle but no sufficiently clear framework identifies which actor answers for a privacy violation, a faulty output, a discriminatory result or an unsafe deployment. This article therefore asks whether existing legislation can be adapted or whether a separate framework for artificial intelligence in healthcare is required.

III. Research objectives

The first objective is to identify the legal and ethical risks created by artificial intelligence in healthcare and to explain why conventional liability law does not fully cover them.[9]

---

[6] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance* (2021); Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, 2024 O.J. (L, 2024/1689).

[7] Scherer, *supra* note 1; Anat Lior, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*, 46 Mitchell Hamline L. Rev. 1043 (2020).

[8] J.K.C. Kingston, *Artificial Intelligence and Legal Liability*, in Research and Development in Intelligent Systems XXXIII 269 (Max Bramer & Miltos Petridis eds., Springer 2016); Nadia Banteka, *Artificially Intelligent Persons*, 58 Hous. L. Rev. 537 (2021).

[9] Herbert Zech, *Liability for AI: Public Policy Considerations*, 22 ERA Forum 147 (2021).

 [ISSN 2581-5369]

The second objective is to examine the rules on patient data privacy, consent and record use, with particular attention to digital health systems and to the handling of previous patient records.[10]

The third objective is to analyse how algorithmic bias can produce discrimination in access to healthcare, in diagnosis and in treatment, particularly where datasets reflect social or demographic skew.[11]

The fourth objective is to assess the legal routes for attributing liability in cases of misdiagnosis, defective software design, unsafe deployment or negligent clinical reliance.[12]

The fifth objective is to propose a liability framework that balances innovation against patient safety, accountability and redress.

The sixth objective is to compare Indian and international regulatory approaches in order to identify a realistic model of governance.

IV. REVIEW OF LITERATURE

The scholarship on artificial intelligence liability offers a doctrinal overview of the technology, its classifications and its legal implications. Its central question is not whether artificial intelligence is technically effective but whether the existing legal regime can attribute liability when artificial intelligence causes damage. Kumar's survey of that field draws together the work of Scherer, Kingston, Lior, Banteka, Zech and Truby.[13] Those writers treat liability as the primary regulatory mechanism, because artificial intelligence is amenable neither to punishment nor to a conventional assessment of subjective fault.[14]

A second theme is transparency and the governance of autonomous systems. The WORLD HEALTH ORGANIZATION treats explainability, predictable behaviour and the provision of information in real time as conditions of trustworthy deployment.[15] Explicability and predictability matter for any autonomous system, but they matter most where the system acts upon vulnerable users. In healthcare both the patient and the practitioner need to understand the

[10] The Digital Personal Data Protection Act, 2023, *supra* note 3; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119) 1 (General Data Protection Regulation), arts. 5, 6, 9.
[11] WORLD HEALTH ORGANIZATION, *supra* note 6.
[12] Lior, *supra* note 7; Scherer, *supra* note 1.
[13] Kumar, *supra* note 4.
[14] Scherer, *supra* note 1; Kingston, *supra* note 8; Lior, *supra* note 7; Banteka, *supra* note 8; Zech, *supra* note 9; Jon Truby, Rafael Dean Brown, Imad Antoine Ibrahim & Oriol Caudevilla Parellada, *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications*, 13 EUR. J. RISK REG. 270 (2022).
[15] WORLD HEALTH ORGANIZATION, *supra* note 6.

 [ISSN 2581-5369]

reasoning behind an algorithm's conclusion. Without it, a diagnosis cannot be challenged and due care cannot be demonstrated.

A third theme is privacy and data governance. The spread of connected devices has increased the generation, storage and processing of data and has created new privacy problems. In healthcare those problems are more acute, because records hold sensitive material: personal identifiers, medical history, occupational data, genetic information, reproductive data and lifestyle data. The literature on artificial intelligence and privacy asks that the law do more than prohibit disclosure. It must also control secondary use, excessive retention and unlawful profiling.[16]

A fourth theme is discrimination and fairness. Work on algorithmic accountability and on responsible artificial intelligence shows that a facially neutral system can perform in a discriminatory way where its training data or its operating environment are not equitable.[17] In healthcare that produces erroneous diagnosis, underdiagnosis of groups underrepresented in the dataset, and divergent risk scores across populations. Fairness, justice and accountability are legal concerns here, and not merely ethical ones.

A fifth theme is the emerging literature on responsible artificial intelligence and regulatory sandboxes. Truby and his co-authors argue for a sandbox approach alongside a regime of strict liability.[18] Governance frameworks of the kind proposed by Dignum argue for a principles-based approach at the design stage.[19] Both are useful, because innovation in healthcare requires iterative testing, and that testing must be conducted under controlled conditions with accountability for adverse outcomes.

The health-sector scholarship completes the picture. James Shaw, Frank Rudzicz, Trevor Jamieson and Avi Goldfarb treat artificial intelligence as an implementation problem in health systems, concerned with changes to care processes and with the design of public health and health services.[20] That work anchors the present analysis in healthcare practice rather than in artificial intelligence theory, and it supports the view that liability must be studied together with implementation, since it is at the point of deployment that liability becomes a live legal question.

[16] Regulation (EU) 2016/679, *supra* note 10, arts. 5, 6, 9; The Digital Personal Data Protection Act, 2023, *supra* note 3, ss. 4-8.
[17] VIRGINIA DIGNUM, RESPONSIBLE ARTIFICIAL INTELLIGENCE: HOW TO DEVELOP AND USE AI IN A RESPONSIBLE WAY (Springer 2019); WORLD HEALTH ORGANIZATION, *supra* note 6.
[18] Truby et al., *supra* note 14.
[19] Dignum, *supra* note 17.
[20] Shaw et al., *supra* note 2.

 [ISSN 2581-5369]

The literature is consistent on one point. Artificial intelligence is not, in law, a neutral tool. It is a high-stakes decision-making setting, and it requires the law to regulate design, use, supervision and remedy as a single legal process. The gap that survey exposes persists in healthcare, where the consequences of error are immediate and often permanent.[21]

V. RESEARCH METHODOLOGY

This article uses a doctrinal method with an analytical orientation. Doctrinal method suits the enquiry because the subject matter is the interpretation of legal rules, case law, regulatory frameworks and policy. Kumar's study adopts the same method, its purpose being to state and analyse the law as it is and as it ought to be.[22] This article follows that method but confines it to the legal questions arising in healthcare.

The research relies on secondary sources, including the primary material collected in that study, official legislative texts, regulatory guidance and the leading literature.[23] The approach is qualitative rather than quantitative. It examines how the law operates in practice, what change is required if legal standards are to accommodate artificial intelligence, and how responsibility is to be distributed along the artificial intelligence supply chain. A comparative element is included, because the question cannot usefully be answered from Indian law alone; developments in the European Union and the guidance of the WORLD HEALTH ORGANIZATION inform the analysis.

The analysis concentrates on six parameters drawn from that literature: patient privacy, patient consent, algorithmic bias and discrimination, misdiagnosis, liability, and previous patient records. Each is treated both as a legal issue and as a question of clinical governance. The object is not to test a hypothesis against field data but to ask whether the existing legal regime is theoretically competent to govern the principal uses of artificial intelligence in healthcare, and where it falls short.

The argument proceeds problem by problem. It identifies a legal issue, marshals the legal materials that bear on it, assesses whether those materials are adequate, and proposes a regulatory solution. That structure suits an emerging technology, where law ordinarily responds only after harm has occurred. The analysis is accordingly directed at anticipating liability rather than at allocating it after the event.

[21] Kumar, *supra* note 4.
[22] Kumar, *supra* note 4.
[23] Kumar, *supra* note 4.

 [ISSN 2581-5369]

VI. Scope and limitations

This article is confined to healthcare liability and regulation. It does not undertake a technical analysis of any artificial intelligence system, nor an empirical study of hospitals and health systems. Its conclusions are therefore legal and policy oriented, and are offered to inform the development of legal policy.

VII. Legal framework

In India the legal framework governing artificial intelligence in healthcare is incomplete and disjointed, spread across several data protection instruments of which the Digital Personal Data Protection Act, 2023 is the principal one.[24] The Act sets out the rights of individuals in relation to the collection and processing of their data, including the right to obtain a summary of the personal data being processed and of the processing activities, the right to correction, completion, updating and erasure, and the right to a readily available means of grievance redressal.[25] Those rights matter for artificial intelligence, which characteristically consumes large volumes of personal health information. The Act supplies a workable foundation for data privacy, but it does not resolve the questions artificial intelligence raises about model explainability, bias assessment, or liability for clinical conclusions. NITI Aayog has identified healthcare as one of the priority sectors for artificial intelligence in India, but its national strategy is a discussion paper and creates no obligations.[26]

The Health Data Management Policy and consent architecture of the Ayushman Bharat Digital Mission are of equal importance. The policy, issued by the National Health Authority, emphasises security and privacy by design, limits on collection and use, and a consent-manager architecture.[27] That is directly relevant where past patient data is used to train or to query a model: health data is to be shared only to the extent necessary, and in accordance with law and with the consent framework.

The Mental Healthcare Act, 2017 matters for confidentiality. It confers a right to confidentiality in respect of mental health, mental healthcare and treatment, extends that right to information held in electronic or digital form, and gives a person with mental illness the right to access their basic medical records.[28] The Act is directed at the treatment of mental illness, but its treatment

[24] Kumar, *supra* note 4.
[25] The Digital Personal Data Protection Act, 2023, *supra* note 3, ss. 11-13.
[26] NITI Aayog, *National Strategy for Artificial Intelligence #AIForAll* (Discussion Paper, June 2018).
[27] National Health Authority, *supra* note 5.
[28] The Mental Healthcare Act, 2017, No. 10 of 2017, ss. 23-25, India Code (2017).

 [ISSN 2581-5369]

of digitally stored medical data is a useful precedent for artificial intelligence systems that process psychological, counselling or behavioural data.

In criminal law, the Bharatiya Nyaya Sanhita, 2023, like the Penal Code before it, predicates liability on a human actor possessing the required mental element.[29] It contains no provision addressing artificial intelligence or software, and it follows that an artificial intelligence system cannot itself be an accused. Ordinary principles of negligence continue to apply to human actors, so that where a practitioner is negligent, or a hospital fails to supervise a tool properly, the human decision-maker remains central to any liability enquiry.

International instruments are moving faster than Indian legislation on the point. The WORLD HEALTH ORGANIZATION treats ethics and human rights as central to both policy and practice.[30] The European Union's Artificial Intelligence Act, Regulation (EU) 2024/1689, entered into force on 1 August 2024 and applies in phases.[31] It does not treat health-related artificial intelligence as high-risk as a class. A system is high-risk under Article 6(1) where it is, or is a safety component of, a product covered by the Union harmonisation legislation listed in Annex I and subject to third-party conformity assessment, which captures software qualifying as a medical device; and Annex III separately captures systems used by or on behalf of public authorities to evaluate eligibility for essential public services including healthcare, and systems used to classify emergency calls or to establish priority in the dispatch of emergency first response services, including emergency healthcare triage.[32] For systems that are high-risk, the Act requires a risk management system, data governance, transparency towards users and human oversight.[33] The direction of travel is clear enough: artificial intelligence in healthcare is to be governed more comprehensively than consumer technology.

VIII. CASE ANALYSIS

Justice K.S. Puttaswamy (Retd.) v. Union of India[34] is the constitutional starting point for privacy in India. Its significance for healthcare artificial intelligence lies in the recognition of informational privacy as a facet of the fundamental right to life and personal liberty. Any system that processes patient data therefore raises a constitutional question as well as a statutory one.

[29] The Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code (2023).
[30] WORLD HEALTH ORGANIZATION, *supra* note 6.
[31] Regulation (EU) 2024/1689, *supra* note 6, art. 113.
[32] Regulation (EU) 2024/1689, *supra* note 6, art. 6(1), annex I, annex III, pt. 5(a), (d).
[33] Regulation (EU) 2024/1689, *supra* note 6, arts. 9, 10, 13, 14.
[34] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

 [ISSN 2581-5369]

Jacob Mathew v. State of Punjab[35] remains the leading authority on medical negligence, for its statement of the standard of care expected of a medical practitioner and of the threshold of gross negligence required before criminal liability attaches. The case says nothing about software. Its reasoning nevertheless suggests that a practitioner could not escape liability by pleading that a computer program directed the course taken, since the exercise of human judgment cannot be set aside in the course of treatment, and least of all where the material before the clinician expresses probabilities rather than certainties.

Indian Med. Ass'n v. V.P. Shantha[36] established that medical services rendered for consideration are 'service' for the purposes of consumer law, so that deficiency in them is actionable before a consumer forum. Where injury involves artificial intelligence, a patient harmed by negligent use of such a service may be able to frame a claim not only in tort but also as deficiency in service, depending on the facts and on the forum.

Suchita Srivastava v. Chandigarh Admin.[37] is significant for personal autonomy and for the requirement of consent. The case concerns reproductive autonomy and does not address diagnostic tools, but the principle it applies supports the argument that a patient should be told when artificial intelligence materially influences diagnosis, triage or treatment. Consent cannot be meaningful if the patient does not know that an automated system is operating on highly sensitive medical information.

Taken together, these decisions show that Indian law already holds the building blocks of liability but no rule allocating it in the healthcare artificial intelligence setting. The present difficulty is interpretive and institutional: the existing principles must be connected to a workflow that identifies the responsibilities of the developer, the deployer and the clinician.

IX. Critical analysis

The difficulty with the present law is not a total absence of legislation but the absence of a clear model of allocation. Artificial intelligence in healthcare introduces causal chains more complex than those familiar to negligence. Where a model is trained on skewed data, validated on a narrow population, and then used by a physician with inadequate supervision, fault is present at several levels at once. A test that looks only for the last human decision-maker will not deter unsafe systems, and a test that fixes the developer alone with liability is too simple to match the facts.

[35] *Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1.
[36] *Indian Med. Ass'n v. V.P. Shantha*, (1995) 6 SCC 651.
[37] *Suchita Srivastava v. Chandigarh Admin.*, (2009) 9 SCC 1.

 [ISSN 2581-5369]

Patient privacy and consent require close scrutiny, because healthcare artificial intelligence is frequently trained and validated on historical patient records. Those records are useful for prediction, and their misuse carries a serious risk. A governing framework should require that records be used only for a specified purpose, that notice be given, that privacy be actively managed, that data be retained only for a limited period, and that every access by an artificial intelligence system leave an audit trail.[38]

Algorithmic bias is an equally serious concern. Bias need not arise from any intention; it may be a property of the system. Where a dataset reflects unequal access to care, or the demographic composition of a particular population, the model learns those patterns. Bias in healthcare can therefore produce concealed discrimination. Liability rules should accordingly treat bias audits and subgroup validation as compliance duties.[39]

Misdiagnosis is the sharpest example of harm, because it bears directly on life and on treatment. The law must distinguish between recommendations that carry inherent clinical uncertainty and those that are plainly unsafe by reason of defective design or inadequate validation. Not every adverse outcome is a legal wrong. Liability should arise where a foreseeable risk is disregarded, where safety measures are omitted, or where human oversight is required in law or in clinical practice and is absent.[40]

X. EMERGING ISSUES AND CONTEMPORARY DEVELOPMENTS

The first development is the growing treatment of healthcare artificial intelligence as a high-risk regulatory category. The European Union's Artificial Intelligence Act is the clearest current example, since it subjects clinical applications, principally those that qualify as medical device software, to a more demanding regime than general consumer software.[41] Its significance extends beyond Europe, because it indicates the direction of global regulation: healthcare artificial intelligence is to be tested and controlled rather than simply placed on the market.

A second development is the expanding body of guidance from the WORLD HEALTH ORGANIZATION. In January 2024 it issued guidance on large multi-modal models in health, following its 2021 guidance on the ethics and governance of artificial intelligence for health.[42]

[38] The Digital Personal Data Protection Act, 2023, *supra* note 3, ss. 4-8; NATIONAL HEALTH AUTHORITY, *supra* note 5.
[39] WORLD HEALTH ORGANIZATION, *supra* note 6.
[40] Zech, *supra* note 9.
[41] Regulation (EU) 2024/1689, *supra* note 6, art. 6(1), annex I.
[42] WORLD HEALTH ORGANIZATION, *Ethics and Governance of Artificial Intelligence for Health: Guidance on Large Multi-Modal Models* (Jan. 18, 2024); WORLD HEALTH ORGANIZATION, *supra* note 6.

 [ISSN 2581-5369]

The message is consistent. Health systems should encourage innovation, but with human involvement, responsible data governance and accountability.

A third development is the maturing of India's digital health ecosystem through the AYUSHMAN BHARAT DIGITAL MISSION. Its consent-manager model and its privacy-by-design policy show health data governance moving from generic privacy protection towards system-level consent management.[43] That model can be adapted for artificial intelligence, so that every access to a record, to a training dataset or to a prediction pipeline is traceable.

A fourth development is the shift from statements of artificial intelligence ethics to actual auditability. Hospitals and technology suppliers are increasingly asked to produce records, to give reasons for what the system does, and to show that the model has been tested on realistic data.

A further development, which this article endorses, is the acceptance that legal responsibility should be assigned in layers. The developer answers for design defects, training errors and undisclosed bias. The hospital answers for procurement, implementation, monitoring and the training of staff. The clinician remains responsible for the exercise of sound judgment, and for not following an unsafe output without question.

XI. FINDINGS AND SUGGESTIONS

A. Findings

Artificial intelligence in healthcare has already demonstrated gains in efficiency, speed and diagnostic reach, but legal practice has not adapted to the risk environment it creates. Kumar's study is right that liability remains unresolved, and the point has particular force in healthcare, where error causes bodily injury and not merely economic loss.[44]

Patient data privacy is fundamental to honest deployment. Artificial intelligence cannot lawfully be deployed unless patient data is held securely, retained properly and used only for a specified purpose. Consent must be clear, informed and readily revocable, and particularly so where records are reused for model training or for secondary reference.[45]

Algorithmic bias has legal consequences that go beyond the ethical objection. Bias produces unequal treatment and obstructs timely diagnosis and access for disadvantaged groups. It must

[43] NATIONAL HEALTH AUTHORITY, *supra* note 5.
[44] Kumar, *supra* note 4.
[45] The Digital Personal Data Protection Act, 2023, *supra* note 3; Regulation (EU) 2016/679, *supra* note 10.

 [ISSN 2581-5369]

be addressed early, because it is difficult to detect from outputs alone once it has been built in at the design and training stages.[46]

Liability for misdiagnosis must now be analysed in layers. A physician cannot escape liability merely because the tool relied upon was an artificial intelligence system, nor can a developer avoid the consequences of an unsafe model. The hospital or other entity that brings the technology into service must answer for a failure to validate, to monitor, and to train staff before deployment.[47]

Previous patient records carry both legal and evidential value and a corresponding risk to privacy. Access to them should be controlled through access restrictions, limits on the purposes for which they may be used, audit trails, and a clear rule requiring a lawful basis and notice to the patient whenever the data is used to train an artificial intelligence system.

B. Suggestions

On the strength of those findings, the following recommendations are offered.

India should frame healthcare-specific rules for artificial intelligence, aligned with the Digital Personal Data Protection Act, 2023 and with the AYUSHMAN BHARAT DIGITAL MISSION framework.

An institution that deploys artificial intelligence in clinical care should prepare and preserve a governance file containing validation reports, risk assessments, bias evaluations and incident logs.

A supplier of an artificial intelligence product should disclose the limitations of the model and its known modes of failure.

Strict requirements of human oversight should attach to any high-risk clinical application.

Patients should be informed of the ways in which artificial intelligence systems affect their care.

A calibrated liability regime should be introduced. Negligence principles can govern low-risk settings, while in high-risk healthcare settings a rebuttable presumption of institutional liability would be more effective, since the patient is not in a position to identify the technical cause of an adverse outcome.

[46] WORLD HEALTH ORGANIZATION, *supra* note 6.
[47] Lior, *supra* note 7; Truby et al., *supra* note 14.

 [ISSN 2581-5369]

XII. Conclusion

Artificial intelligence is altering healthcare within a legal environment designed for an older kind of medical practice. That mismatch is what makes liability the central regulatory question. As the literature shows, the problems of liability, transparency and regulation are general, but they present themselves most acutely in healthcare, where privacy, informed consent, bias, diagnosis and medical history bear directly on patient wellbeing.

The existing legal framework governs parts of the field but not the whole of it. Data protection law addresses some privacy violations, medical negligence law addresses some clinical errors, and consumer protection law affords compensation in some situations. None of them produces a complete scheme of accountability for artificial intelligence. A workable healthcare-specific regime must therefore combine legal obligations, clinical standards, auditability and human control.

The most defensible approach is a layered model of accountability, which fixes the developer with responsibility for defects in design and training, the hospital for failures of deployment and monitoring, and the physician for improper use and excessive reliance. Such a model can keep pace with innovation while leaving a real route to legal accountability. If the law can make artificial intelligence in healthcare open to scrutiny, to testing and to challenge, the technology can improve care without eroding patient rights.

*****

 [ISSN 2581-5369]