INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE IN HEALTHCARE: LIABILITY AND ACCOUNTABILITY

AUTHORED BY - PRABHJOT KAUR[1]

ABSTRACT

The integration of Artificial Intelligence (AI) into modern healthcare promises a revolution in diagnostic accuracy, predictive analytics, and personalized treatment. However, its autonomous nature poses significant legal and ethical challenges, particularly concerning liability and accountability for adverse outcomes. The deployment of AI introduces new risks of clinical inaccuracies and data breaches, where a single error can have devastating consequences for vulnerable patients. This article confronts the challenge of assigning legal blame and accountability for medical errors originating from artificial intelligence. Despite these concerns, a clear regulatory framework to govern AI in medicine is notably absent. The analysis concludes that current regulations are insufficient, necessitating proactive legal reforms and clear accountability structures. This paper therefore underscores the urgent need for appropriate guidelines, emphasizing transparency in AI systems, stringent data privacy norms, and strengthened cybersecurity safeguards to protect all stakeholders.

Keywords:- *Artificial Intelligence, healthcare, liability, accountability, regulatory framework*

INTRODUCTION

Recent advances have shown that AI-powered healthcare tools can match or even surpass human clinicians in performing specific medical tasks. The primary motivation for introducing AI into patient diagnosis is to help solve pressing global health challenges. These include the growing shortage of medical professionals, exacerbated by ageing populations, and the need to improve access to quality care in underserved, low-resource regions. Despite this promising potential, the integration of AI must be approached with caution, as healthcare is a highly complex and safety-critical field where any technological failure can result in direct harm to patients.

[1] Assistant Professor, CT Group of Institutions, Shahpur Campus, Jalandhar

ISSN: 2582-6433

The need for Artificial Intelligence in the world arose at the times of COVID 19. At that time, the world level healthcare systems faced challenges like lack of access to doctors and hospitals, excessive wastage of basic healthcare facilities along with rising population. This COVID period in actual senses caused strain on our existing healthcare system. It was felt due to shortage of personal equipment, insufficient and inaccurate diagnostic tests, overburdened clinicians etc. There has to be something which could improve the flaws.

AI emerged as a useful and reliable tool in healthcare. It, in many senses, have improved the efficiency and patient care leading to an increase in patient satisfaction and follow up. Besides these, certain limitations and pitfalls regarding the usage of AI in healthcare have to be considered before blindly trusting upon the same. The growing use of AI in clinical decisions challenges existing norms and raises doubts about how healthcare providers can meet their legal duties. For this, it is essential to know about how the AI have emerged in the field of healthcare.

THE EVOLUTION OF ARTIFICIAL INTELLIGENCE: FROM CONCEPT TO CLINIC

Artificial Intelligence, or AI, is the science of building smart machines that can think and act on their own. The idea started in the 1950s when a scientist named Alan Turing asked if a machine could ever think like a human. This goal became official at a famous summer Dartmouth conference in the year 1956, where experts believed that one day, machines could be as smart as people.[2]

Early industrial AI aimed to replicate human actions, leading to inventions like the first robotic arm in 1955 and "Eliza," a 1964 chatbot that simulated conversation[3]. A major breakthrough was "Shakey," a robot that could understand and execute human commands, proving AI's practical potential.

AI entered the world of medicine in the 1970s. Early computer programs like INTERNIST-1 could help figure out what disease a patient had based on their symptoms.[4] This development

[2] Cordeschi, R. (2007). AI turns fifty: Revisiting its origins. *Applied Artificial Intelligence*, 21(4-5), 259–279.
[3] M.E. Moran, Evolution of robotic arms. *J. Robot. Surg.* 2007, 1, 103–111.
[4] Laboratory of Computer Science, "DXplain", *available at:* http://www.mghlcs.org/projects/dxplain (last visited on Nov. 1, 2025).

ISSN: 2582-6433

generated significant academic and governmental interest. Soon, tools like MYCIN helped doctors choose the right antibiotics, and DXplain offered even more diagnostic help.[5]

From the 2000s to today, AI has grown tremendously. IBM's Watson computer showed it could understand human language and find answers in huge amounts of data, later helping to research complex diseases. Now, AI has now become an integral component of contemporary healthcare practice, used in tools like Pharmbot to educate patients, proving its journey from a simple idea to a helpful, everyday reality.[6]

According to Hamid, AI systems are capable of synthesizing and analyzing extensive medical datasets from diverse origins. This capability facilitates disease detection and provides valuable insights to guide clinical decisions.[7] Using large amounts of medical data, AI can find hidden patterns. This helps create new treatments and better ways to manage healthcare. However, we need more research to prove AI works well and to find all its uses. A major challenge, as expert Gerke points out, is figuring out who is to blame when an AI system causes harm to a patient. For example, a recent investigation found that a company's AI was giving hospitals wrong medical advice for very sick patients. This shows the real danger: if an AI makes a mistake and suggests a doctor skip a test, it could lead to a delayed diagnosis and hurt the patient[8]. Right now, there are no clear laws for this kind of situation. It is hard to know who is responsible: the doctor, the hospital, or the company that made the AI. This problem is made worse by the "black box" issue, which means we often cannot understand how the AI reached its decision.

[5] C.A. Kulikowski, "Beginnings of Artificial Intelligence in Medicine (AIM): Computational Artifice Assisting Scientific Inquiry and Clinical Art—With Reflections on Present AIM Challenges" 28 *Yearb. Med. Inform.* 249 (2019).
[6] Bakkar, N., Kovalik, T., Lorenzini, I., Spangler, S., Lacoste, A., Sponaugle, K., Ferrante, P., Argentinis, E., Sattler, R., & Bowser, R. (2018). Artificial intelligence in neurodegenerative disease research: Use of IBM Watson to identify additional RNA-binding proteins altered in amyotrophic lateral sclerosis. Acta Neuropathologica, 135(2), 227–247. https://doi.org/10.1007/s00401-017-1785-8
[7] Sobia Hamid, "The Opportunities and Risks of Artificial Intelligence in Medicine and Healthcare" (2016), *available at:* https://www.cuspe.org/wp-content/uploads/2016/09/Hamid_2016.pdf (last visited on Oct. 31, 2025).
[8] Casey Ross, "Epic's AI Algorithms, Shielded from Scrutiny by a Corporate Firewall, Are Delivering Inaccurate Information on Seriously Ill Patients" *STAT*, July 26, 2021, *available at:* https://www.statnews.com/2021/07/26/epic-hospital-algorithms-sepsis-investigation/ (last visited on Nov. 1, 2025).

ISSN: 2582-6433

UNDERSTANDING MEDICAL NEGLIGENCE AND A DOCTOR'S DUTY OF CARE

The rules for deciding if a doctor was medically negligent come from an old legal precedent. To prove negligence, one must show three things: there is a standard, "usual" way to treat a condition; the doctor did not follow that standard way; the action the doctor took was one that no reasonably skilled doctor would have taken[9]. The idea that doctors have a "duty of care" towards their patients is another basic legal rule. This means doctors must act carefully to avoid causing harm that could be foreseen[10]. In short, they are legally required to provide care that meets a proper standard to keep their patients safe. This duty also includes telling patients about the important risks of a treatment so the patient can give informed consent.

So, what is the "proper standard" of care? It is known as the Bolam test[11]. This test says a doctor is not negligent if their actions are supported by even a small group of other reasonable medical professionals. It doesn't matter if some other doctors would have done something different. However, the law has since evolved. In a later case called Bolitho[12], the court added that the accepted medical practice a doctor follows must also be logical and reasonable. A court can now reject a doctor's defense if the expert opinions supporting them are illogical or don't make sense. This means that simply saying "other doctors would have done the same" is not always enough if the action itself was unreasonable.

Furthermore, the law has established that a doctor can meet their duty of care by consulting a senior colleague[13]. A key question now is whether using an AI system for assistance could fulfill this same legal duty. The legal standard is based on a "reasonable professional" who avoids both excessive caution and overconfidence[14]. AI could potentially help doctors achieve this balanced judgment. Furthermore, the law requires doctors to obtain informed consent by explaining significant risks to patients[15]. As AI is used more in medicine, this duty expands: doctors must now also explain the risks of using AI itself. However, this is challenging because AI-related risks can be difficult to identify and communicate. This difficulty could prevent patients from giving truly informed consent and expose them to new harms, highlighting the

[9] *Hunter v Hanley* (1955) 213 SLT
[10] *Donoghue v Stevenson* [1932] AC 562
[11] *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582
[12] *Bolitho v City and Hackney Health Authority* [1997] 4 All ER 771
[13] *Willsher v Essex Area Health Authority* [1988] 1 AC 1074
[14] *Glasgow Corporation V Muir* [1943] 2 AC 448
[15] *Montgomery v Lanarkshire Health Board* [2015] UKSC 11

ISSN: 2582-6433

urgent need for legal standards to adapt to the age of AI.

Indian jurisprudence has historically evolved to align medical negligence standards with shifting professional norms. A landmark shift occurred in *Jacob Mathew v. State of Punjab*, where the Supreme Court established that negligence is measured against the benchmarks of an ordinary competent professional[16]. Critically, the Court distinguished between civil and criminal liability, stipulating that the latter necessitates a significantly higher threshold of gross recklessness. This legal bifurcation is particularly pertinent in the realm of AI-integrated medicine, where adverse outcomes often stem from intricate human-machine dynamics rather than clear-cut individual misconduct. Furthermore, contemporary liability has expanded toward an institutional model; hospitals now bear an independent duty of care regarding the selection, implementation, and monitoring of the medical technologies they deploy[17].

As AI systems become more pervasive in clinical settings, the law faces a pivotal dilemma: does AI reliance constitute valid professional support or an unauthorized delegation of medical discretion? While physician collaboration is a long-standing practice, reliance on algorithms is legally defensible only when the practitioner maintains substantive oversight and can interpret the AI's logic[18]. Conversely, as these technologies become industry standards, the failure to utilize them may eventually be viewed as a deviation from the acceptable standard of care. This evolution also redefines informed consent, requiring doctors to disclose the use of AI, its inherent limitations, and the risk of algorithmic error[19]. Given the "black box" complexity of such systems, maintaining detailed audit trails and prioritizing explainability are essential for legal transparency. Ultimately, while patients retain the right to reject AI-driven interventions, the legal system must urgently modernize the traditional duty of care to address the unique accountability challenges posed by autonomous medical technology[20].

WHO IS LIABLE WHEN AI CAUSES HARM IN HEALTHCARE?

The increasing use of Artificial Intelligence in healthcare raises difficult questions about legal responsibility when AI-driven decisions cause patient harm. Traditional legal doctrines such as

[16] *Jacob Mathew v. State of Punjab* (2005) 6 SCC 1.
[17] *Spring Meadows Hospital v. Harjol Ahluwalia*, (1998) 4 SCC 39
[18] S. Gerke, T. Minssen & G. Cohen, "Ethical and Legal Challenges of Artificial Intelligence-Driven Healthcare", 29 *Cambridge Quarterly of Healthcare Ethics* 1 (2020).
[19] *Samira Kohli v. Dr Prabha Manchanda*, (2008) 2 SCC 1.
[20] *Samira Kohli v. Dr Prabha Manchanda*, (2008) 2 SCC 1.

ISSN: 2582-6433

vicarious liability and product liability provide possible frameworks, but neither fits neatly with the autonomous and opaque nature of modern AI systems. Under vicarious liability, a hospital or healthcare institution may be held responsible for errors committed by AI tools used in diagnosis or treatment, treating the AI as an extension or agent of the institution. However, this approach becomes problematic where the AI is developed by third-party companies and operates with limited human control, making it difficult to determine whether the harm resulted from improper use by clinicians or inherent flaws in the technology itself.

Product liability offers an alternative approach by shifting responsibility toward AI developers and manufacturers. If an AI system is defective in its design, training data, or warning mechanisms, the developer may be liable for the resulting harm. In theory, this aligns with consumer protection principles, particularly where hospitals rely on AI systems without the capacity to evaluate their internal logic. Yet, applying product liability to self-learning AI remains challenging, as identifying a specific defect in a constantly evolving algorithm is complex. Traditional protections such as the learned intermediary doctrine, which places responsibility on doctors as informed decision-makers, may also lose relevance where AI systems generate recommendations with minimal scope for meaningful clinical intervention[21]. The integration of AI further complicates the existing duty and standard of medical care. As AI tools become widely accepted and demonstrably superior in certain tasks, their use may itself become part of the expected standard of care, potentially rendering failure to use such technology negligent. At the same time, clinicians may be required to inform patients about the role of AI in their treatment as part of informed consent. This creates tension between reliance on advanced technology and the clinician's obligation to exercise independent professional judgment, particularly when AI recommendations conflict with traditional medical practice.

Given these complexities, liability may increasingly shift away from individual doctors toward healthcare institutions and AI developers. Holding clinicians personally responsible for AI errors is arguably unjust, especially when the decision-making processes of AI systems are inaccessible or incomprehensible[22]. Healthcare institutions are better placed to manage risks through system audits, governance protocols, and insurance mechanisms, while developers may bear greater responsibility under evolving product liability regimes. Emerging regulatory

[21] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, [1985] *OJ L 210/29*.
[22] Consumer Protection Act, 2019, ss. 2(10), 83; G. Sartor & A. Omicini, "The Responsibility Gap in Artificial Intelligence and the Law", 27 *Artificial Intelligence and Law* 1 (2021).

ISSN: 2582-6433

models, particularly in the European Union, suggest a future in which AI software is treated as a product, easing the burden on patients to prove negligence and enhancing transparency obligations for developers. This shift reflects an effort to align legal accountability with the realities of AI-driven healthcare.

PATIENT SAFETY, DATA SECURITY, AND SYSTEMIC RISKS OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE

The integration of Artificial Intelligence into clinical decision-making introduces significant risks of clinical inaccuracies that extend far beyond mere technical errors. Unlike conventional software failures, AI inaccuracies directly affect diagnosis, treatment choices, and patient outcomes, thereby posing serious threats to patient safety. A critical concern is the absence of systematic reporting on the downstream clinical consequences of AI errors, such as delayed interventions, incorrect prognoses, or inappropriate medication prescriptions.[23]This lack of transparency obscures the true risk profile of AI systems in healthcare and undermines evidence-based evaluation of their safety. Recent empirical studies on generative AI applications in medicine reveal alarmingly high rates of fabricated or "hallucinated" medical information, which, if relied upon by clinicians, can result in misdiagnosis and preventable harm.[24] The vulnerability is particularly acute in high-stakes environments such as oncology, emergency medicine, and intensive care units, where erroneous recommendations can be fatal. A further challenge lies in the "black box" nature of many advanced AI systems, particularly those based on deep learning architectures. These systems often produce outputs without providing intelligible explanations for how conclusions are reached, making it difficult for clinicians to meaningfully evaluate or challenge AI-generated recommendations.[25] As scholars have observed, when explainability is absent, human oversight risks being reduced to a superficial validation exercise, commonly described as "automation bias" or "rubber-stamping," where clinicians defer to AI outputs despite uncertainty.[26] This erosion of professional judgment not only weakens accountability but also disrupts traditional medico-legal frameworks that assume decisions are based on discernible reasoning. Without explainable AI, courts may struggle to assess negligence, causation, and foreseeability of harm,

[23] W. Price & I. Cohen, "Privacy in the Age of Medical Big Data", 25 *Nature Medicine* 37 (2019).
[24] J. Nori et al., "Capabilities of GPT-4 on Medical Challenge Problems", *arXiv* (2023); *see also* M. Harrer, "Attention Is Not All You Need: Hallucinations in Medical AI", *BMJ Health & Care Informatics* (2023).
[25] F. Doshi-Velez & B. Kim, "Towards a Rigorous Science of Interpretable Machine Learning", *arXiv* (2017).
[26]K.C.R. Parasuraman & V. Riley, "Humans and Automation: Use, Misuse, Disuse, Abuse", 39 *Human Factors* 230 (1997).

ISSN: 2582-6433

thereby complicating patient access to remedies.

Beyond clinical inaccuracies, AI-driven healthcare systems significantly amplify cybersecurity and data protection risks. Healthcare databases contain highly sensitive personal and genetic information, making them prime targets for cyberattacks such as ransomware, data breaches, and identity theft.[27] Successful cyber intrusions can disrupt hospital operations, compromise AI training datasets, and lead to inaccurate clinical outputs, thereby endangering patient lives. The legal ramifications of such breaches are substantial, as healthcare providers and technology developers are subject to stringent data protection obligations under regulatory frameworks such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States.[28] Inadequate cybersecurity safeguards may therefore result not only in patient harm but also in significant legal and financial penalties.

These technological vulnerabilities disproportionately affect patients, who remain the most exposed stakeholders in AI-enabled healthcare systems. Patients often lack awareness that AI tools are being used in their diagnosis or treatment and are rarely informed of the associated risks, including data misuse or algorithmic error.[29] This asymmetry of knowledge undermines patient autonomy and informed consent, particularly where AI systems continuously learn from personal health data. Ethical and legal scholars emphasize that safeguarding patients requires embedding privacy-by-design principles, mandatory risk disclosures, robust cybersecurity standards, and effective human oversight into AI governance frameworks.[30] Without such protections, the promise of AI-driven healthcare risks being overshadowed by systemic vulnerabilities that compromise trust, safety, and fundamental patient rights.

GLOBAL REGULATORY FRAMEWORKS GOVERNING ARTIFICIAL INTELLIGENCE IN HEALTHCARE

Across jurisdictions, regulators have begun to recognize the transformative yet high-risk nature of Artificial Intelligence in healthcare, prompting the development of dedicated governance frameworks. The European Union has taken the most comprehensive approach through the

[27] ENISA, *Cybersecurity Threat Landscape for Health Sector* (European Union Agency for Cybersecurity, 2022).
[28] General Data Protection Regulation (EU) 2016/679; Health Insurance Portability and Accountability Act, 1996 (US).
[29] *Samira Kohli v Dr Prabha Manchanda*, (2008) 2 SCC 1.
[30] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO 2021).

ISSN: 2582-6433

enactment of the EU Artificial Intelligence Act, 2024, which expressly categorizes AI systems used in medical diagnosis, treatment, and patient management as "high-risk."[31] Such systems are subject to stringent pre-market conformity assessments, continuous post-market monitoring, mandatory human oversight, and strict transparency obligations. By embedding patient safety and accountability into binding legislation, the EU model seeks to proactively mitigate harm while fostering responsible innovation, offering a structured liability environment for both healthcare providers and AI developers.

In the United States, regulation of AI in healthcare has evolved primarily through sector-specific oversight rather than comprehensive legislation. The Food and Drug Administration (FDA) regulates AI-based medical software under its medical device framework, focusing on safety, effectiveness, and real-world performance monitoring.[32] The FDA has issued guidance on Software as a Medical Device (SaMD) and adaptive machine-learning systems, emphasizing lifecycle regulation, post-deployment surveillance, and algorithmic updates.[33] However, liability questions in the US largely continue to be addressed through tort law and product liability doctrines, resulting in a fragmented approach where accountability is often determined ex post through litigation rather than ex ante regulatory clarity.

In contrast, India's regulatory approach to AI in healthcare remains largely aspirational and policy-driven, with limited enforceable legal standards. While NITI Aayog's National Strategy for Artificial Intelligence identifies healthcare as a priority sector and promotes AI adoption to improve access and efficiency, it does not articulate a clear liability or accountability framework for AI-induced harm.[34] The absence of sector-specific legislation leaves existing laws, such as the Consumer Protection Act, 2019 and the Medical Devices Rules, 2017, to operate in a fragmented and often inadequate manner when applied to autonomous and adaptive AI systems. Furthermore, recent enactments like the Digital Personal Data Protection Act, 2023 address data governance but remain silent on clinical accountability and patient remedies for AI-related errors.[35] This regulatory vacuum creates uncertainty for innovators, healthcare institutions, and patients alike, underscoring the urgent need for India to move beyond policy

[31] European Union, *Artificial Intelligence Act*, Regulation (EU) 2024.
[32] US Food and Drug Administration, *Artificial Intelligence and Machine Learning in Software as a Medical Device* (FDA 2021).
[33] US Food and Drug Administration, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device* (2019).
[34] NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (Government of India 2018).
[35] Digital Personal Data Protection Act, 2023 (India)

ISSN: 2582-6433

statements toward a coherent legal framework that balances innovation with patient safety and legal certainty.

DEVELOPING A COMPREHENSIVE LEGAL FRAMEWORK FOR ACCOUNTABILITY IN AI-DRIVEN HEALTHCARE

The development of a legally sustainable framework for Artificial Intelligence in healthcare requires a clear and structured allocation of liability among the multiple actors involved in AI-assisted medical decision-making. Traditional negligence principles, which focus primarily on individual clinicians, are inadequate for addressing harms arising from complex human–machine interactions. A modern accountability regime must therefore delineate the respective duties of doctors, healthcare institutions, and AI developers, ensuring that responsibility is assigned in proportion to control, knowledge, and capacity to prevent harm. Such clarity would reduce uncertainty for healthcare professionals while strengthening patient protection by ensuring that liability does not unfairly rest on actors with limited influence over AI system design or functioning.

Equally central to AI accountability is the principle of transparency and patient autonomy. Mandatory disclosure of AI use in diagnosis or treatment is essential to meaningful informed consent, particularly where algorithmic recommendations significantly influence clinical outcomes. Patients must be informed not only of the involvement of AI systems but also of their limitations, potential risks, and the extent of human oversight. In parallel, independent auditing mechanisms are necessary to monitor algorithmic accuracy, bias, and safety over time, especially for adaptive AI systems that evolve after deployment. Regular audits and impact assessments can serve as preventive tools, reducing the likelihood of systemic harm and strengthening trust in AI-enabled healthcare.

Beyond liability and transparency, ethical governance and effective remedies must form the backbone of any accountability framework. Professional medical bodies and regulatory authorities should adopt binding ethical guidelines governing the appropriate use of AI, reinforcing principles of fairness, non-discrimination, and human oversight. At the remedial level, the introduction of a no-fault compensation mechanism for AI-related medical harm would ensure timely patient relief without the need for complex and prolonged litigation over

ISSN: 2582-6433

fault and causation.[36] Such a model, already familiar in certain healthcare contexts, aligns with the public interest in patient safety and social justice. Collectively, these measures can ensure that innovation in healthcare proceeds without undermining fundamental rights, ethical standards, or public confidence in medical institutions.

CONCLUSION

In conclusion, while Artificial Intelligence has the potential to fundamentally transform healthcare delivery by enhancing diagnostic accuracy, efficiency, and accessibility, its integration into clinical practice presents profound legal and ethical challenges that existing frameworks are ill-equipped to address. The opaque nature of AI systems, the multiplicity of actors involved, and the heightened risks to patient safety and data privacy demand a rethinking of traditional doctrines of medical negligence and liability. Comparative regulatory experiences demonstrate that proactive, sector-specific governance, rather than reliance on post hoc litigation, is essential to ensure accountability and public trust. For India, the absence of a dedicated legal framework governing AI in healthcare creates uncertainty for clinicians, institutions, innovators, and patients alike. This study underscores the urgent need for a coherent, rights-oriented legal approach that clearly allocates responsibility, mandates transparency and informed consent, strengthens institutional oversight, and provides accessible compensation mechanisms for AI-related harm. By aligning technological innovation with constitutional values, patient welfare, and global best practices, India can ensure that the deployment of AI in healthcare remains both ethically sound and legally resilient, ultimately serving the broader objective of sustainable and equitable public health advancement.

[36] UK Law Commission, *Liability for Autonomous Systems* (Consultation Paper No 229, 2021).