



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

REGULATING ARTIFICIAL INTELLIGENCE IN MEDICAL ERRORS: CRIMINAL LIABILITY APPROACHES IN INDIA AND THE EUROPEAN UNION

Kannirasu S.

2nd Year LL.M.

Department of Law, Central University of Tamil Nadu

ABSTRACT

AI is a powerful and transformative area in computer science, and its influence is expanding rapidly across all other professions, particularly in healthcare. AI in healthcare refers to the use of advanced algorithms and machine learning models to analyse complex medical data and support clinical decisions. However, as AI use grows in medical practice, mistakes made by these systems can seriously harm patients. When such errors occur, it is unclear who should face criminal responsibility. This raises the issue of liability, as the lack of a specific criminal liability framework creates a legal vacuum. Traditional criminal law frameworks are based on the twin principles of *actus reus* and *mens rea*, which require proof of intention, knowledge, recklessness, or negligence. The application of these principles becomes problematic when harm is caused not directly by a human actor, but by an autonomous or semi-autonomous AI system. This study finds a gap; India currently has no laws criminalising liability for AI-caused errors. This study aims to determine who is responsible when AI causes medical errors, with the help of the EU AI Act, and to establish an emergency policy or act in this age of AI in India; criminal responsibility must be reconstructed through doctrines such as *corporate criminal liability*, *vicarious liability*, and *product liability* principles among developers, healthcare institutions, and medical practitioners. This study employs a doctrinal research methodology and analyses the European Union's legal framework. This research helps clarify AI ethics, criminal law, and healthcare regulations, providing guidance for courts and policymakers dealing with AI-related medical errors in India.

Keywords: *Artificial intelligence, Medical errors, Criminal liability, EU AI Act, Legal vacuum*

1. INTRODUCTION

"Artificial intelligence" is a general term that covers systems that perform tasks that typically require human intelligence, such as sensing, thinking, decision-making, and learning. In healthcare, this includes algorithms that analyse images, monitor vital signs, recommend treatments, or even perform tasks using robots. These systems can range from closely watched tools to more independent or even fully autonomous ones.¹ In recent years, AI has become a very important element in healthcare. In the modern medical landscape, AI refers to the use of algorithms and machine learning models to analyse multifaceted data, thereby identifying errors and supporting clinical decisions. AI refers to the use of smart computer systems to analyse large amounts of medical data, reports, scans, and patient histories. These systems help doctors make better, faster decisions about diagnosis and treatment. Even though AI is highly accurate and useful, it is advancing so quickly that the laws and regulations governing its use in healthcare are still not fully developed. As autonomous and semi-autonomous systems begin to make choices once reserved for human practitioners, the occurrence of medical errors introduces a profound legal crisis due to a legal vacuum.² In traditional criminal law, Responsibility is based on two key principles: *actus rea* (the wrongful act) and *mens rea* (the guilty intention). To establish criminal liability, it must be proven that a human acted with intention, knowledge, recklessness, or negligence.³ However, when harm is caused by an autonomous AI system. Many modern AI and machine learning systems are hard to understand. Their decisions come from complicated models that often don't make sense to humans. The opacity of AI systems may also create difficulties in identifying the basis of an automated medical decision and determining responsibility when harm occurs.⁴ This creates a major issue in fixing responsibility. The study highlights a gap in the Indian legal system: there are currently no specific laws that clearly establish criminal liability for AI-caused medical errors. This research aims to determine who is responsible when AI causes harm in healthcare, using the European Union AI Act, 2024, as a benchmark.⁵ The EU's approach can guide India in developing AI laws for healthcare. Since there are no specific laws in place, criminal responsibility must be reconstructed by applying **Corporate Criminal Liability, Vicarious**

¹ Saksham, Artificial Intelligence and Criminal Liability in Healthcare: Issues & Challenges, 7 Int'l J. Multidisciplinary Res. (2025).

² Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* 34-37 (Springer 2013).

³ *Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1.

⁴ Saksham, *supra* note 1, at 2.

⁵ 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 1689) 1.

Liability, and Product Liability. This study suggests a framework to help courts and policymakers handle AI-related issues in healthcare.

2. STATEMENT OF PROBLEM

The central problem of this research is the lack of clarity regarding liability when a medical practitioner uses an AI system that causes harm to a patient. While AI supports doctors in making critical decisions, it creates a legal vacuum because current Indian law does not specify where a doctor's responsibility ends and a developer's or a hospital's responsibility begins. This confusion makes it difficult for courts to decide who is responsible: the doctor, the developer, or the hospital that deployed the system. Without a clear framework, such as the one proposed in the EU AI Act, to distribute responsibility through doctrines like corporate and product liability, the legal system cannot effectively resolve cases of AI-driven medical errors.

3. RESEARCH OBJECTIVE

This study aims to analyse how the "black-box" nature of AI affects traditional criminal law principles, specifically how the lack of transparency in algorithms makes it difficult to prove *actus rea* (the wrongful act) and *mens rea* (the guilty intention). To examine the Indian legal standards for medical negligence, such as the Jacob Mathew precedent, and determine why they are insufficient to address errors caused by autonomous AI systems. To evaluate the risk-based regulatory framework of the European Union Artificial Intelligence Act, 2024 and assess whether it can be adapted as a model for Indian healthcare laws. Ultimately, this paper aims to identify the legal vacuum and suggest legal reforms that, through corporate criminal liability, vicarious liability, and product liability, address issues affecting developers, hospitals, and practitioners.

4. RESEARCH METHODOLOGY

This study uses a doctrinal research method, through which the analysis of statutes and judicial precedents is conducted. It adopts a comparative approach, comparing the Indian legal system with the European Union's Artificial Intelligence Act (Regulation (EU) 2024/1689) to identify gaps and propose legal reforms to address AI-related medical errors.

5. DECONSTRUCTING THE LEGAL FRAMEWORK: THE "BLACK BOX" CHALLENGE TO CRIMINAL JURISPRUDENCE

Many modern AI and machine learning systems are hard to understand. Their decisions come from complicated models that often don't make sense to humans. This "black-box" nature makes it hard to know how decisions are made, which makes it difficult to find out what went wrong and who is to blame. For example, there is a known problem in the literature regarding

the balance between explainable and accountable decision-making.⁶ Normally, when medical negligence occurs, it is easy to understand how the mistake happened. But AI systems, especially deep learning models, operate through complex algorithms in ways that are unclear to humans. The main problem in applying traditional criminal law to AI-related medical errors is the “black-box” nature of AI.

5.1. The Crisis of *Mens Rea* under the BNS, 2023

Under the Bharatiya Nyaya Sanhita (BNS), criminal liability remains anchored in the individual’s “guilty mind”. When an AI system provides a faulty diagnosis, the traditional requirements of intent or knowledge cannot be established within the software itself.⁷ Recent analysis suggests that AI lacks consciousness and moral values, so it cannot have mens rea; it is also not a legal person. Because of this, it becomes difficult to take legal action against developers or doctors under section 106(1) of the BNS when unexpected errors are caused by autonomous AI systems.⁸

5.2. The Autonomy Gap and De-Individualisation

Unlike traditional medical tools, AI can act autonomously to some extent. This independence breaks the usual connection between the person who created the tool and the action it takes. So, if the AI selects a harmful treatment due to biased data or unexpected changes in its system, the developer can argue that they did not anticipate or know the mistake would occur.⁹ This leads to a De-Individualisation of liability, where responsibility spreads among doctors, hospitals, and developers, so no single person can be clearly blamed, potentially resulting in a failure of justice for the patient.

5.3. Failure of *Jacob Mathew* Standard

The “reasonable professional” test in *Jacob Mathew* assumes that only a human doctor makes the decision.¹⁰ However, when a reasonably competent doctor relies on a reliable AI tool, and it fails due to a hidden error in the system, it does not clearly indicate who is responsible. As argued by Shreya and Gowshiha (2026), Indian law does not yet have a proper system for

⁶ Saksham, supra note 1, at 2.

⁷ Artificial Intelligence and Criminal Liability: Challenges under the Bharatiya Nyaya Sanhita, 2023, 13 TIJER – Int’l Res. J. 3 (Mar. 2026).

⁸ Maitri Singh, Medical Device Failures in India – Determining the Liability, SCC OnLine (Feb. 10, 2025).

⁹ Najam Khaliq, Mohammad Nasir, Samreen Ahmed & Kaif Siddiqui, The Role of Artificial Intelligence in Improving the Public Health Care Delivery System in India: A Legal-Ethical Audit, 51(1) *Indian Journal of Community Medicine* 32–41 (2026), https://doi.org/10.4103/ijcm.ijcm_7_25.

¹⁰ *Jacob Mathew*, supra note 3

addressing decisions made jointly by humans and AI, underscoring the need for urgent changes in medical liability laws.¹¹

6. COMPARATIVE ANALYSIS: THE EU AI ACT'S DISTRIBUTION OF LIABILITY

While Indian law struggles to determine whether the developer or the doctor is responsible, the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) provides a clear system of shared responsibility. It focuses not just on punishing mistakes after they happen, but also on preventing risks in advance by treating AI as a system in which duties are shared among different parties, rather than as a simple tool.¹²

6.1. Liability of the "Provider" (The Developer)

The EU framework identifies the "provider" as the person or company responsible for ensuring that the AI system is safe and transparent. Under Article 6 of the EU AI Act, 2024, medical AI is considered "high-risk" and must undergo strict safety checks before it can be used.¹³ If a medical error occurs due to a design defect, algorithmic bias, or a failure in transparency, the Provider is held liable under the principles of Strict Product Liability. This means the company cannot escape responsibility by saying the system is a "black box" or too complex to understand.

6.2. Liability of the 'Deployer' (The Doctor/Hospital)

On the other hand, the "deployer" (the doctor or hospital) is responsible for properly using and monitoring the AI system during its operation. Article 14 mandates a "Human-in-the-Loop" (HITL) requirement, ensuring that the AI is designed to be overseen by natural persons.¹⁴ From a criminal law perspective, this avoids the "autonomy gap." If a doctor fails to properly monitor the AI or ignores its warnings, the responsibility remains with the doctor for failing in their duty of care.

6.3. Solving the Causation Gap through Logging

A critical contribution of the EU Act to criminal evidence is its mandate for automatic event logging (Article 12).¹⁵ In the event of a patient's death, these records function like a "digital black box." They help investigators determine whether the mistake was due to a problem in the AI system (blaming the provider) or to improper use by the doctor or hospital (blaming the deployer), thereby addressing the current lack of clear evidence in Indian law.

¹¹ Shreya S. & Gowshiha A., Legal Accountability for AI Errors in Life-Saving Medical Decisions: Medical Negligence, Liability and Data Protection under Indian Law, 9 Int'l J. Health & Med. L. (2026).

¹² *Regulation (EU) 2024/1689, supra note 5, arts. 16, 26.*

¹³ *Id.* art. 6.

¹⁴ *Id.* art. 14.

¹⁵ *Id.* art. 12.

7. RECONSTRUCTING LIABILITY

To address the “legal vacuum” in India, this study suggests a three-level criminal approach. Instead of blaming only the doctor, the law should share responsibility among the developer, the hospital, and the doctor, depending on the type of mistake.

7.1. Corporate Criminal Liability for AI Providers

Corporate criminal liability is a legal doctrine that treats a company as a "juristic person," allowing it to be prosecuted for crimes just as a human being can. In the context of medical AI, this means that if an error occurs because a company knowingly sold a defective or biased algorithm, the company can be criminally held responsible. Under the Bharatiya Nyaya Sanhita (BNS), 2023, the term "person" specifically includes companies and associations, meaning they are not immune from criminal law. Since a company lacks a body or mind, Indian courts apply the Identification Doctrine (also known as the Alter Ego theory). This means the guilty mind (*mens rea*) of top managers or directors who decided to use the faulty AI is treated as the company's guilty mind. In the landmark case of *Standard Chartered Bank v. Directorate of Enforcement*, the Supreme Court of India established that a corporation can be prosecuted for offences even if the law mandates imprisonment.¹⁶ Since a company cannot be sent to jail, the court imposes a heavy criminal fine instead. In this framework, this ensures that when a "Black-Box" error kills a patient, the AI developer cannot hide behind the complexity of their code to escape justice.

7.2. The Doctrine of Vicarious Liability for Hospitals

Currently, hospitals often escape criminal liability for their doctors' mistakes. However, if a hospital uses an AI system without proper “Human-in-the-Loop” safeguards (human supervision), it should be held vicariously liable. In this context, the hospital can be seen as the “master” that selects and uses the “digital agent” (the AI system). If the hospital does not provide doctors with proper training on how to control or override the AI, then the hospital management should be held responsible for “Institutional Negligence”.¹⁷

7.3. Professional Negligence and the 'Override' Duty

For the individual doctor, the standard from Jacob Mathew should be updated. A doctor should be held criminally liable only if they deliberately ignore an AI warning or fail to properly supervise the system as required under a proposed “AI Healthcare Act.” If the doctor correctly

¹⁶ *Standard Chartered Bank v. Directorate of Enforcement*, (2005) 4 SCC 530.

¹⁷ Saksham, *supra* note 1, at 6.

follows a certified AI system, but it fails due to a hidden error, the doctor should not be blamed, and responsibility should shift back to the developer (provider).¹⁸

8. JUDICIAL RESPONSE: FROM TRADITIONAL NEGLIGENCE TO THE AI "MENACE"

The development of medical negligence law in India aims to protect doctors' professional judgment while also ensuring they are accountable for their actions. However, recent judicial warnings about the use of Artificial Intelligence have added a new level of responsibility for both legal and medical professionals.

8.1. The Traditional Standard: *Jacob Mathew v. State of Punjab*

The landmark case of *Jacob Mathew v. State of Punjab* (2005) remains the "Gold Standard" for medical negligence in India.¹⁹ The Supreme Court established that a doctor cannot be prosecuted for every error of judgment, but only for "gross negligence." The court emphasised that a professional is only expected to exercise an "ordinary degree of skill" and should not be harassed by frivolous criminal proceedings. This study argues that in the AI era, a doctor's reliance on an unverified algorithm could potentially cross the line from a simple "error of judgment" to "gross negligence" if they fail to perform independent verification.

8.2. Adherence to Protocol: *Kusum Sharma v. Batra Hospital*

In *Kusum Sharma v. Batra Hospital* (2010), the Court held that if a doctor follows a recognised and accepted medical practice, they cannot be held liable just because the treatment did not succeed.²⁰ If a hospital makes the use of an AI tool part of its standard procedure, and the doctor properly follows it, then responsibility for any failure should shift from the doctor to the hospital or the developer who created the AI.

8.3. The 2026 Warning: The "Menace" of Unverified AI

In a landmark development in March 2026, the Supreme Court of India in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*²¹ The trial court judge relied on fabricated or non-existent judgments generated by an AI tool, demonstrating that the risks associated with generative AI are not confined to lawyers or litigants but may also arise within the judicial process. The incident highlights the importance of independently verifying judgments, case citations and legal authorities before relying upon AI-generated legal material in judicial proceedings.

¹⁸ Regulation (EU) 2024/1689, *supra* note 5, art. 14.

¹⁹ *Jacob Mathew*, *supra* note 3.

²⁰ *Kusum Sharma & Ors. v. Batra Hospital & Medical Research Centre*, (2010) 3 SCC 480.

²¹ *Gummadi Usha Rani v. Sure Mallikarjuna Rao*, 2026 SCC OnLine SC 341 (Feb. 27, 2026).

A separate issue arose in the hearing concerning *Mercy vs. Mankind* on 17 February 2026 before a bench headed by the Chief Justice. This matter should not be conflated with the *Gummadi* incident. The *Gummadi* matter concerned the use of fabricated AI-generated judgments by a trial court judge, whereas *Mercy vs. Mankind* involved a separate Public Interest Litigation (PIL) hearing concerning the issues raised before the Supreme Court. These developments demonstrate the broader need for caution, transparency and human verification when AI-generated information is used in the legal system.

The incidents, therefore, illustrate that AI should function as an assistive tool rather than a substitute for independent legal verification. Whether the reliance on AI-generated material occurs through a lawyer or a judge, the ultimate responsibility for ensuring the authenticity and accuracy of legal authorities must remain with the human decision-maker.

A doctor can also be held responsible for acting on incorrect AI diagnoses. Under this approach, blindly trusting an AI system is not a valid defence to avoid liability for professional negligence.

9. RECOMMENDATION

Based on a comparative analysis of the EU AI Act and recent judicial warnings in India, this study suggests a two-part approach to address the current legal vacuum.

9.1. Practical Suggestions

Medical practitioners should follow the principle of “**Algorithmic Scepticism**,” meaning they should not blindly trust AI. As highlighted in *Gummadi Usha Rani v. Sure Mallikarjuna Rao*²² The duty to verify information always remains with the human. AI should be treated only as a second opinion, and the final medical decision must always be confirmed by the doctor. For healthcare institutions, hospitals should follow a “**Human-in-the-Loop**” (HITL)²³ approach. This means no high-risk AI system should work on its own; a qualified doctor must always supervise it and have the authority to override its decisions at any time. **Ethical Considerations and Patient Autonomy:** Patients should be clearly informed when AI is used in their diagnosis or treatment. They must give proper consent, with an understanding of AI's role in their care.²⁴ For developers, AI providers should focus on “**Explainable AI**”, which means making AI systems more transparent and easy to understand. The “black-box” nature of algorithms should be reduced so that their decisions can be clearly explained and properly reviewed when errors occur.

²² *Gummadi Usha Rani*, *supra* note 21.

²³ *Regulation (EU) 2024/1689*, *supra* note 5, art. 14.

²⁴ Saksham, *supra* note 1, at 7.

9.2. Suggestion for Legal Reforms

India should introduce an **“AI Healthcare Act,”** based on the **European Union Artificial Intelligence Act (Regulation (EU) 2024),**²⁵ which treats medical AI as “high-risk.”²⁶ This law should require **automatic event logging**²⁷ so that all AI actions are recorded, creating a “digital trail” that can serve as evidence in the event of errors. Secondly, the **Bharatiya Nyaya Sanhita, 2023,** should be amended by inserting an Explanation for algorithmic negligence under **Section 106(1)** to include **“algorithmic negligence.”** This would make it possible to take action against companies under corporate criminal liability when a death is caused by defects in AI design or biased data.

10. CONCLUSION

The use of AI in healthcare has created a **“legal vacuum” in which traditional criminal law concepts such as actus reus and mens rea struggle to address** errors made by autonomous systems. The “black-box” nature of AI makes it difficult to assign responsibility, leaving patients at risk when something goes wrong. By analysing the EU AI Act (2024)²⁸ and the Indian Supreme Court’s warning in *Gummadi Usha Rani*,²⁹ It is clear that responsibility cannot be shifted to machines. In the future, Indian medical law must adopt “algorithmic scepticism,” in which doctors remain the final decision-makers. To protect patients, India should adopt a new liability framework that includes corporate criminal liability for developers and vicarious liability for hospitals, ensuring that AI serves as a support tool rather than a replacement for human judgment and accountability.

Three points stand out from this study. First, the problem is not that Indian criminal law is completely silent, but that its tests were written for human beings. Section 106(1) of the BNS and the gross negligence standard in *Jacob Mathew* work well when a doctor makes a mistake personally, but they do not tell us what a doctor, a hospital and a developer owe each other when the mistake comes from an AI system.³⁰ Second, the EU AI Act shows that this gap can be filled by dividing duties in advance. Providers must build safe and transparent systems; deployers must supervise them; and automated logs allow investigators to trace errors to their sources.³¹ Indian courts can draw on this reasoning even before Parliament acts, as the Supreme

²⁵ Regulation (EU) 2024/1689, *supra* note 5.

²⁶ Regulation (EU) 2024/1689, *supra* note 5.

²⁷ Regulation (EU) 2024/1689, *supra* note 5, art. 12.

²⁸ Regulation (EU) 2024/1689, *supra* note 5.

²⁹ *Gummadi Usha Rani*, *supra* note 21.

³⁰ *Jacob Mathew*, *supra* note 3.

³¹ Regulation (EU) 2024/1689, *supra* note 5, arts. 12, 14, 16, 26.

Court has already held that a company can be prosecuted and fined for criminal offences.³² Third, the judiciary has made it clear that human professionals cannot hide behind technology. If a lawyer or a judge must verify what AI produces, a doctor who acts on an AI diagnosis without any independent check can hardly claim to have met the standard of ordinary skill and care.³³

At the same time, this study does not argue that every AI failure should lead to punishment. Criminal law should be used only where there is knowledge, recklessness or gross negligence, such as selling a system known to be biased, deploying it without training the staff, or ignoring its warnings. Where a certified system fails despite proper use, responsibility should move to the developer, and civil compensation may be the better remedy. A balanced law of this kind will protect patients without discouraging doctors and hospitals from using technology that can save lives.

Future research can test this framework against actual cases once Indian courts begin to decide AI-related medical negligence claims, and can also study how product liability rules interact with criminal responsibility. Until such a law is passed, the safest course is simple: AI may assist, but the human professional, the hospital and the developer must each answer for their own part.

³² *Standard Chartered Bank*, *supra* note 16.

³³ *Gummadi Usha Rani*, *supra* note 21.