# AN ANALYSIS OF CRIMINAL LIABILITY ARISING FROM THE USE OF ROBOTICS IN THE MEDICAL FIELD IN INDIA

Reshav Jain, CHRIST (Deemed To be) University, Delhi NCR

## 1. ABSTRACT

Although the use of robotics in medicine, especially in autonomous surgery, has revolutionized healthcare delivery, it also makes it more difficult to enforce liability in cases of negligence. However, while the Indian legal system still functions in a vacuum, other jurisdictions around the world have started to create a framework for determining who is responsible for harm caused by robotics systems—developers, operators, or institutions.

The question of whether criminal liability can be imposed in cases involving autonomous medical robots is currently not sufficiently addressed by Indian law. This raises important issues regarding the level of care that the robots must provide during surgery, the potential for establishing mens rea, and the division of responsibility between the human and the robot.

By conducting doctrinal research, analyzing the legal framework's suitability to handle the current situation—which includes cases involving the liability of the robots performing the surgery—and examining comparative legal approaches from other countries' legal frameworks, the researcher aims to close that gap. By doing this, it also hopes to aid in the creation of a logical legal framework that strikes a balance between medical robotics accountability and technological innovation.

**Keywords:** Medical Field, Health Care, Robotics, Criminal Liability, Negligence, Autonomous Surgery.

## 2. Statement of Problem

Robotics' quick adoption in medicine has revolutionized healthcare delivery by enabling previously unheard-of levels of surgical precision and efficiency. But when negative consequences arise, this technological breakthrough also presents difficult moral and legal questions. In contrast to conventional medical malpractice cases, where a surgeon or other healthcare professional can be held directly accountable, robotic interventions conflate the roles of software developers, manufacturers, human actors, and the autonomous system itself. The current Indian legal system, which is based on mens rea theories and established standards of care, is still unclear about how criminal liability should be assessed in cases where robotic surgeries cause harm. On the other hand, some foreign jurisdictions have started looking into accountability models for autonomous systems, highlighting India's lack of readiness to handle these issues. In addition to putting patients at risk, the lack of clear legal guidelines discourages innovation because it is unclear who is responsible for what. Therefore, using comparative insights from international practices, this study aims to address the urgent question of how criminal responsibility can and should be distributed in cases involving medical robotics within the Indian context.

## 3. Research Methodology

The present research adopts a doctrinal and comparative legal research approach to analyze the criminal liability of robotics in the medical field, particularly in the Indian context. Since medical robotics represents a rapidly evolving technological frontier, the study relies primarily on secondary sources, such as statutes, judicial precedents, academic commentaries, government policy papers, and international guidelines.

### 1. Nature of Research

This research is qualitative and analytical in nature. It does not involve empirical or field-based study but instead relies on a critical examination of existing legal provisions, doctrinal interpretations, and comparative jurisprudence.

### 2. Sources of Data

- Principal Sources: Articles 21 and 47 of the Constitution, as well as statutory provisions like the Drugs and Cosmetics Act, the Medical Device Rules, and the Bharatiya Nyaya

Sanhita, 2023 (BNS).

- Secondary Sources: Scholarly articles, reports like NITI Aayog's "Responsible AI for All," international policy documents, and commentary on medical law, robotics, and criminal jurisprudence. We'll also look at Indian and international case laws pertaining to medical malpractice, liability, and AI ethics.

### 3. Evaluation by Comparison

By looking at the legal stances in other jurisdictions, including the US (FDA regulatory framework and tort law), the UK (medical negligence and corporate liability principles), and the EU (AI Act), the study takes a comparative approach. The goal of this cross-jurisdictional approach is to find potential models or protections that the Indian legal system could adopt.

### 4. Study Scope

The scope is restricted to examining the criminal liability aspect of robotics in medical practice, with particular attention to mens rea, strict liability, standard of care, and responsibility attribution in cases of injury or death resulting from autonomous or semi-autonomous robotic surgeries. Although acknowledged, ethical issues will only be discussed insofar as they have an impact on criminal responsibility.

**Limitations**

Hospitals, practitioners, or patients are not empirically surveyed in this study. Additionally, except in cases where it is necessary to make distinctions from criminal law, it does not address the civil or contractual liability of robotics in medical practice. Comparative references are only used for analytical enrichment, and the analysis is limited to the Indian legal context.

## 4. Research Questions

1. What doctrinal and practical gaps arise when applying traditional principles like mens rea and actus reus to autonomous or semi-autonomous medical systems, and how well does the current Indian legal framework handle criminal liability arising from the use of robotics in the medical field?

2. What standards of liability are most appropriate to ensure both fairness and accountability in cases of medical harm caused by robotic systems, and how should criminal responsibility be distributed among stakeholders, including surgeons, hospitals, manufacturers, and programmers?

3. What comparative lessons can India draw from the legal approaches of jurisdictions such as the United States, the United Kingdom, and the European Union, and how can these insights lead towards the development of a forward-looking legal framework that balances patient safety, accountability, and technological innovation in medical robotics?

## 5. Research Objectives

1. To determine doctrinal and practical gaps in applying traditional principles like mens rea and actus reus to autonomous or semi-autonomous medical systems, and to critically evaluate the suitability of the current Indian legal framework in addressing criminal liability arising from the use of robotics in the medical field.

2. To establish liability standards that preserve equity, accountability, and patient safety; and to decide how much criminal responsibility should be divided among important parties, such as surgeons, hospitals, manufacturers, and programmers, in cases of medical harm brought on by robotic systems.

3. To examine the comparative legal systems of the US, UK, and EU in order to draw practical conclusions for India and aid in the creation of a forward-thinking legal system that guarantees patient safety, upholds accountability, and promotes ethical technological advancement in medical robotics.

## 6. Literature Review:

1. **Robotics in Health Care: Who is Liable? – Dr Vikrant Yadav, School of Law, Ajeenkya D. Y. Patil University, Pune**

   **Citation:** Yadav, Vikrant. (2018). Robotics in Health Care: Who is Liable?. SSRN Electronic Journal. 10.2139/ssrn.3598028.

   **Link:**https://www.researchgate.net/publication/341983975_Robotics_in_Health_Care_W

ho_is_Liable

**Essence of the paper:** The article examines the rise of robotics and AI in healthcare, noting benefits like precision surgeries but stressing legal challenges in assigning liability for malfunctions. Currently, responsibility falls on manufacturers, providers, or users, with debate over granting robots legal personhood. It calls for clear laws and liability frameworks to ensure safety and accountability as technology advances.

**Research Gap or Limitation:** The paper notes a gap in legal frameworks for healthcare robotics, as current laws, including in India, do not address accountability for harm from autonomous systems. Non-recognition of robots as legal persons hinders liability attribution, and global regulation is absent. This underexplored area calls for standardised laws and models like Gabriel Hallevy's framework to ensure safety and clarity in automated healthcare.

2. **Medical Liability Issues (and Beyond) Resulting from the Use of New Technologies - Massimo Farina**

**Citation:** Farina, Massimo & Palladino, Alessia. (2023). Medical Liability Issues (and Beyond) Resulting from the Use of New Technologies. 10.1007/978-3-031-32625-7_4.

**Link:**https://www.researchgate.net/publication/373224004_Medical_Liability_Issues_and_Beyond_Resulting_from_the_Use_of_New_Technologies

**Essence of the paper:** The essence of this research paper is that rapid technological advancements in healthcare particularly in artificial intelligence, robotics, telemedicine, and digital health services are transforming the traditional doctor–patient relationship and the delivery of medical care. This transformation raises critical legal, ethical, and deontological questions, especially concerning civil and criminal liability, accountability, data protection, and the redistribution of responsibility between healthcare professionals and institutions. The paper examines the Italian legal framework, analyzing how these innovations challenge core pillars of the healthcare relationship trust, accountability, and professional responsibility while also exploring the ethical implications of introducing artificial agents into healthcare.

**Research Gap or Limitation:** The paper compares Italy's and India's legal approaches to

healthcare technologies, noting that India lacks dedicated AI, robotics, and telemedicine laws, with patient rights and informed consent in AI-assisted care undefined. Both countries face gaps in AI-related liability case law, and issues like bias, data protection, cybersecurity, and IP remain unaddressed, alongside ethical concerns over reduced human involvement.

3. **FIXING CRIMINAL LIABILITY AS PER ELEMENTS OF A CRIME: A REVIEW IN MODERN ERA OF AI AND ROBOTICS By D R Mahmood, Mahmood Ahmed Shaikh, Bahria University**

   **Citation:** Mahmood, D & Shaikh, Mahmood & Shafiq, D & Rahman, U & Tahir, Prof & Khuharo, Khadim & Shahid, Dr. (2023). FIXING CRIMINAL LIABILITY AS PER ELEMENTS OF A CRIME: A REVIEW IN MODERN ERA OF AI AND ROBOTICS. 4.

   **Link:**https://www.researchgate.net/publication/389633022_FIXING_CRIMINAL_LIABILITY_AS_PER_ELEMENTS_OF_A_CRIME_A_REVIEW_IN_MODERN_ERA_OF_AI_AND_ROBOTICS

   **Essence of the paper:** This paper explores the evolution of criminal liability with AI and robotics, stressing the need for adaptable laws to address challenges posed by systems lacking intent or emotions. It notes that liability often shifts to programmers and operators, and calls for a nuanced, ethical update to criminal law for AI-driven actions.

   **Research Gap or Limitation:** The integration of robotics into India's healthcare system exposes gaps in laws on criminal liability for autonomous medical robots. Current frameworks focus on human responsibility, leaving accountability unclear when robots cause harm. This paper identifies these gaps and proposes principles to regulate liability, balancing accountability with technological progress.

4. **Bharatiya Nyaya Sanhita, 2023 (BNS) drafted by the Ministry of Home Affairs, Government of India.**

   **Citation:** Bharatiya Nyaya Sanhita, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1, 25 Dec. 2023**.**

   **Link:** https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

**Essence of the Statute:** The Bharatiya Nyaya Sanhita, 2023 updates India's criminal law with provisions on cybercrime and corporate liability but lacks specific rules on medical robotics. Relevant sections 106 (death by negligence), 115–118 (hurt by negligent acts), 110 (corporate liability), and 61 (criminal conspiracy) apply only to human actors, leaving a gap in addressing criminal accountability for AI-driven medical harm.

**Limitation:** While the Bharatiya Nyaya Sanhita, 2023 modernises criminal law, it has no provisions for autonomous medical systems, limiting liability to human actors. It's negligence and corporate liability rules suit human conduct, not robot-driven harm, and offer no framework for sharing liability among stakeholders, leaving AI-related accountability unresolved.

**5. Jacob Mathew Vs. State of Punjab and Ors. by Supreme Court of India**

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

**Link:** https://www-manupatrafast-in

christuniversityncr.knimbus.com/pers/Personalized.aspx

**Essence of the Case**: In *Jacob Mathew v. State of Punjab* (2005) 6 SCC 1, the Supreme Court held that criminal liability for medical negligence arises only for gross negligence, applying the *Bolam test* to compare a doctor's conduct with a competent peer. It also required credible medical opinion before prosecution, a standard likely relevant to robot-assisted procedure cases.

**Limitation or Research Gap:** While *Jacob Mathew v. State of Punjab* sets a standard for criminal medical negligence under the *Bolam test*, it presumes a human professional. In medical robotics, harm may stem from autonomous decisions or programming errors, with no direct human action. The case offers no guidance on mens rea, causation, or shared liability among doctors, programmers, and manufacturers, revealing a gap in applying negligence principles to AI-driven medical devices.

**6. Kusum Sharma and Ors. Vs. Batra Hospital and Medical Research Centre and Ors. Decided by the Supreme Court Of India**

**Citation:** Kusum Sharma and Ors. vs. Batra Hospital and Medical Research Centre and

Ors. (10.02.2010 - SC) : MANU/SC/0098/2010

**Link:**https://www-manupatrafast-in-christuniversityncr.knimbus.com/pers/viewDocByManuidPop.aspx?manuid=zwKDa4S8QbBCBSkXPhUPwY5CqQmaAQ/9fT/TmfIpDN/z9G2eCv5mPvwvCjKGvBAE2XniZ8KIilknbfxvqFXqow==

**Essence of the case:** In *Kusum Sharma v. Batra Hospital & Medical Research Centre*, (2010) 3 SCC 480, the Supreme Court held that medical negligence exists only when a doctor's conduct falls below the standard of a reasonably competent professional (*Bolam test*), and mere errors of judgment are insufficient. While protective of both patients and doctors, this standard is difficult to apply to autonomous medical robots, revealing a gap in assessing AI-driven errors.

**Limitation or the Research gap:** The Kusum Sharma ruling assumes a human professional for the Bolam test comparison. In robotics-based care, harm may stem from autonomous decisions or malfunctions, with no direct human conduct to assess. It offers no method to gauge AI "standard of care" or assign liability among designers, operators, and manufacturers, leaving a gap in applying these principles to medical robotics.

7. **Risks of Artificial Intelligence in the Medical Field and Its Legal Implications by Dr. Tamer Hamed Al-Qadi, Professor of Criminal Law, Faculty of Sharia and Law, Islamic University, Others.**

**Citation:** Tamer, Hamed & Al-Qadi, & Law, Criminal & Nisreen, Ibrahim & Kheiri, Murtada. (2025). Risks of Artificial Intelligence in the Medical Field and Its Legal Implications. 2025.

Link:https://www.researchgate.net/publication/393253726_Risks_of_Artificial_Intelligence_in_the_Medical_Field_and_Its_Legal_Implications

**Essence of the paper:** The paper *"Risks of Artificial Intelligence in the Medical Field and Its Legal Implications"* highlights AI's benefits in healthcare and risks like errors, cyberattacks, and ethical issues. It examines criminal and civil liability, administrative oversight, and urges specific regulations, staff training, and stronger controls to address these challenges.

**Limitation or Research Gap:** The paper *"Risks of Artificial Intelligence in the Medical Field and Its Legal Implications"* notes key limitations in addressing criminal liability for medical robotics: proving manufacturing errors is difficult, as seen in Da Vinci Xi robot cases where US courts absolved manufacturers despite faults; there is no specific legislation tailored to AI's unique risks, with current laws focusing on negligence; and liability is framed as solely human-centric targeting manufacturers, operators, or owners without exploring AI legal personhood or direct liability, leaving gaps in adapting criminal law to autonomous systems.

8. **The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability by Fatima Al-Misbah**

**Citation:** Al-Misbah, Fatima. (2024). The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability. International Journal for Scientific Research. 3. 91-114. 10.59992/IJSR.2024.v3n3p3.

**Link:**https://www.researchgate.net/publication/379203444_The_Legal_Personality_of_Robotic_Surgery_and_the_Possibility_of_Determining_Criminal_Liability/citation/download

**Essence of the Paper:** The paper explores the concept of legal personality in the context of robotic surgery, concluding that while civil liability can be assigned to the manufacturer or medical entity, determining criminal liability for the robot itself remains challenging, necessitating specific legislation to define responsibility and regulate its legal status.

**Limitation or Research Gap:** The key limitation of the research is that it remains largely theoretical, as current legal systems including those in the medical field do not recognise robots as having independent criminal liability, making practical application of its proposals uncertain. It does not address jurisdictional variations, existing regulatory frameworks, or real-world case studies, and overlooks the technical and evidentiary challenges in attributing criminal intent or negligence to autonomous medical systems.

9. **Indian Medical Association Vs. V.P. Shantha and Ors. Decided by the Supreme Court of India.**

**Citation:** Indian Medical Association v. V.P. Shantha, (1995) 6 SCC 651.

**Link:https://www-manupatrafast-in-christuniversityncr.knimbus.com/pers/viewDocByManuidPop.aspx?manuid=zwKDa4S8QbBCBSkXPhUPwTgL3tnKDuLaRDyxadNBwfZ8WD/OK5nQaM9k2tK96euveyUchar(43)char(43)aHC54y1FnQKgVl8MQ==**

**Essence of the case:** *Indian Medical Assn. v. V.P. Shantha* (1995) brought medical services under the Consumer Protection Act, making doctors and hospitals vicariously liable for staff actions. Applied to medical robotics, hospitals could be liable for robot-assisted harm under their supervision, though the case does not address fully autonomous systems.

**Limitation of the case:** The ruling in *Indian Medical Association v. V.P. Shantha* focuses on defining "medical services" under consumer protection law and attributing liability to human medical professionals. It does not address scenarios involving autonomous decision-making or malfunctions by medical robots, where no direct human action forms the basis of negligence. The case offers no framework for assessing criminal liability, attributing mens rea, or determining accountability among manufacturers, programmers, and operators in AI-driven medical harm, leaving a gap in applying its principles to robotics in healthcare.

**10. State of Maharashtra Vs. Hindustan Construction Company Ltd. was decided by the Supreme Court of India**

**Citation:** *State of Maharashtra v. Hindustan Construction Co. Ltd.*, (2010) 4 SCC 518.

**Link:**https://www-manupatrafast-in-christuniversityncr.knimbus.com/pers/viewDocByManuidPop.aspx?manuid=zwKDa4S8QbBCBSkXPhUPwY5CqQmaAQ/9fT/TmfIpDN8IXYchar(43)uL8EwhbKKQYCUgnnXqerKult4char(43)AhXlgP2JB8Qhg==

**Essence of the case:** In *State of Maharashtra v. Hindustan Construction Co. Ltd.*, the Supreme Court clarified that corporations can be held criminally liable for offences requiring mens rea through the acts and intentions of their agents. Applied to medical robotics, this principle suggests that if harm is caused by a manufacturing or programming defect, the corporation behind the robot could face criminal liability via vicarious attribution, even though the robot itself lacks legal personhood.

**Limitation of the case:** The judgment in State of Maharashtra v. Hindustan Construction Co. Ltd. supports corporate liability via human intent, but it is ill-suited for autonomous medical robots where harm may occur without direct human action, leaving AI-specific criminal accountability unresolved.

11. **Information Technology Act, 2000, (IT Act, 2000), drafted by the Ministry of Information Technology, Government of India.**

**Citation:** Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

**Link:https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf**

**Essence of the Statute:** The Information Technology Act, 2000, governs electronic records, digital signatures, cybersecurity, and offences related to computer systems, providing a legal framework for regulating digital and network-based activities in India.

**Limitation of the Statute:** The Information Technology Act, 2000, focuses on cybercrimes and data protection, lacking provisions for criminal liability in cases where autonomous medical robots cause physical harm, making it inadequate for addressing negligence or accountability in AI-driven healthcare.

12. **Robotic and Autonomous Systems in a Military Context: The Future is Now, prepare for 2045 by Patrick Bolder, Michel Rademaker, and Bianca Torossian.**

**Citation:** Bolder, P., Rademaker, M., & Torossian, B. (2021). Robotic and Autonomous Systems in a Military Context: The Future is Now, prepare for 2045. Hague Centre for Strategic Studies.

**Link:** http://www.jstor.org/stable/resrep29554.8

**Essence of the article:** The document underscores that, much like in military RAS, autonomous medical robots face unresolved issues of accountability when harm occurs, highlighting the need for clear legal frameworks, meaningful human oversight, and traceability to assign responsibility, especially as such systems make independent, high-stakes decisions.

**Limitations or the research gap of the paper:** The paper reveals key gaps in military robotics, including unclear accountability, legal ambiguities under IHL, technical complexity, lack of intent in machines, and evolving policy norms all of which parallel your focus on criminal liability. While it broadly identifies these challenges, your research seeks to address them by proposing concrete legal frameworks to attribute responsibility for wrongful acts by autonomous systems to relevant human actors or entities.

**13. The Right to Contest AI, by Julie E. Cohen.**

**Citation:** Kaminski ME, Urban JM, 'The Right to Contest AI' (2021) 121 Columbia Law Review 1957

**Link:** https://www.jstor.org/stable/27083420

**Essence of the paper:** The document contrasts EU's proactive frameworks granting individuals the right to contest AI decisions with India's largely procedural and reactive approach, highlighting the need for India especially in medical robotics to adopt systemic accountability measures, clear liability standards, and robust contestation rights to ensure patient safety, redress, and the protection of human dignity.

**Limitation of the article:** The article notes that while the right to contest AI decisions is vital for fairness and transparency, existing frameworks like the GDPR remain vague and lack clear operational models. It highlights research gaps in developing standardised, scalable, and context-sensitive contestation mechanisms that effectively address systemic biases, underscoring the need for more precise, actionable rules to make such rights practically enforceable.

**14. "Civilian Drones and India's Regulatory Response" by Ananth Padmanabhan**

**Citation:** Padmanabhan A, 'Civilian Drones and India's Regulatory Response' (2017) Carnegie Endowment for International Peace.

**Link:** http://www.jstor.org/stable/resrep12772

**Essence of the paper:** The document is on India's drone regulation reveals key lessons for medical robotics: unclear liability, privacy risks, new harms from decentralization, and

outdated, fragmented laws. It urges proactive, unified rules to ensure accountability and protect rights while fostering innovation.

**Limitation or research gap of the paper:** The drone regulation document offers useful parallels for medical robotics, but has key gaps for your focus on criminal liability. It centres on civil law, public-space harms, and simpler operator–manufacturer liability, lacking discussion of medical-specific harms, complex multi-actor culpability, healthcare regulators, and ethical issues like patient autonomy. It also omits the near-total absence of criminal liability precedents in the medical robotics context, making your research challenge even greater.

15. **"Origins of Robotic Surgery: From Skepticism to Standard of Care" by Evalyn I. George, BS, COL Timothy C. Brand, MD and others.**

**Citation:** George EI, Brand TC, LaPorta A, Marescaux J, Satava RM, 'Origins of Robotic Surgery: From Skepticism to Standard of Care' (2018) 22(4) JSLS : Journal of the Society of Laparoendoscopic Surgeons e2018.00039

**Link:** https://doi.org/10.4293/JSLS.2018.00039

**Essence of the Paper:** The document provides a detailed historical and technical account of the evolution of robotic surgery, from early concepts to the widespread adoption of systems like the da Vinci, highlighting key milestones, innovators, and technological advances. However, it does not address legal, ethical, or criminal liability issues, making it useful for contextual background but not directly aligned with your focus on accountability in medical robotics.

**Limitation or the research gap of the paper:** The document offers a rich historical and technical account of robotic surgery's evolution covering milestones, key innovators, and technological advances but entirely omits legal, ethical, or accountability considerations. It provides no discussion of liability, regulatory frameworks, or precedents for harm caused by medical robots, making it useful for background context but irrelevant to the core legal focus of your research on criminal liability in the medical robotics field.

16. **Digital Personal Data Protection Act, 2023 (DPDP Act), drafted by Ministry of Electronics and Information Technology (MeitY) and Government of India**

**Citation:** Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

**Link:**https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

**Essence of the Statute:** The DPDP Act, 2023, safeguards personal data, including sensitive health information processed by AI-driven medical devices. In the context of medical robotics, hospitals, device manufacturers, and software developers become data fiduciaries, obliged to obtain patient consent, ensure data minimisation, and maintain strong security measures. While the Act prescribes heavy administrative penalties for breaches, it does not establish criminal liability for harm caused by AI malfunctions or autonomous decisions, leaving accountability for physical injury outside its scope.

**Limitation of the Statute:** The Digital Personal Data Protection Act, 2023, primarily safeguards personal and health data but remains limited in addressing the criminal liability of robotics in the medical field. While it provides measures against data breaches and imposes administrative penalties, it does not cover cases of physical harm caused by autonomous medical robots or offer guidance on attributing mens rea and allocating liability when AI decision-making directly results in injury.

**17. NITI Aayog – Responsible AI Principles and Medical Robotics, Government of India.**

**Citation:** NITI Aayog, *Responsible AI for All: 2021 Strategy*, Government of India, 2021, available at https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (last visited Aug. 9, 2025).

**Link:** https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf

**Essence of the guidelines:** NITI Aayog's *"Responsible AI for All"* strategy promotes safety, transparency, accountability, and ethics in AI deployment. Applied to medical robotics, these principles would require explainable algorithms, rigorous pre-deployment testing, and continuous monitoring to prevent harm. However, these remain non-binding guidelines and lack enforceable provisions for criminal liability in cases where AI-driven medical devices cause injury, thereby failing to fill the legislative gap in attributing responsibility for autonomous harm.

**Limitation of the guidelines:** The limitation of NITI Aayog's Responsible AI for All: 2021 Strategy lies in its purely advisory nature it sets out ethical principles like safety, transparency, and accountability, but does not establish binding legal obligations or criminal liability mechanisms. As a result, it cannot resolve the key challenge your research addresses: attributing and enforcing accountability when autonomous medical systems cause harm.

**18. Criminal Protection of Public Relations Related to Robots: A Comparative Study by Haider Kazem Hathout, College of Nursing, AlQadisiyah University, Iraq.**

**Citation:** Hathout HK, *Criminal Protection of Public Relations Related to Robots: A Comparative Study* (2024) 19(1) *International Journal of Criminal Justice Sciences* 1.

**Link:** https://ijcjs.com/menu-script/index.php/ijcjs/article/view/793/474

**Essence of the paper:** This research paper broadly explores the risks of robots in military and medical contexts, highlighting concerns like ethical non-compliance, data misuse, malfunctions, and the absence of clear responsibility when robots cause harm. While it calls for strong legal frameworks and even considers questions of robot legal personhood, its medical discussion focuses mainly on patient data violations and safety risks

**Limitation or research gap of the paper:** Hathout (2024) broadly addresses criminal protection related to robots, but omits the specific context of autonomous medical robots in India. It does not engage with India's healthcare laws, medical negligence thresholds, or the unique challenge of assigning criminal liability in AI-driven surgeries. Your paper fills this gap by focusing on how Indian law can adapt to regulate and attribute responsibility for harm caused by medical robotics.

**19. Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges**

**Citation:** Razek, R. M. A. M. A. (2024). Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges. *Journal of Law and Sustainable Development*, *12*(1), e2443

**Link:** https://doi.org/10.55908/sdgs.v12i1.2443

**Essence of the paper:** The paper explores the legal and ethical challenges of assigning criminal responsibility for medical robot errors, noting current laws are ill-suited for autonomous systems and struggle with causation and intent. It considers liability for manufacturers, operators, and programmers, questions robot legal personhood, and calls for new laws and ethical guidelines to ensure patient safety while supporting innovation.

**Limitation or the research gap:** Current global laws, including in India, are rooted in human-centric liability and offer little guidance for harms caused by autonomous medical robots, creating an "accountability vacuum" when no direct human intent or negligence exists. With robots not recognised as legal persons, liability falls on manufacturers, operators, or developers an approach inadequate for India's minimal and outdated medical malpractice and negligence provisions. Given India's unique socio-legal environment and lack of specific regulation, there is a clear need for a dedicated framework to define criminal liability for medical robotics while ensuring accountability and supporting innovation.

**20. The AI-Robotic Prescription: Legal Liability When an Autonomous AI Robot is Your Medical Provider AI Robot is Your Medical Provider, Erika Sophia Grossbard, University of Miami School of Law**

**Citation:** Erika Sophia Grossbard, The AI-Robotic Prescription: Legal Liability When an Autonomous AI Robot is Your Medical Provider, 33 U. MIA Bus. L. Rev. 273 ().

**Link:** https://repository.law.miami.edu/umblr/vol33/iss2/6

**Essence of the paper:** The paper explores legal liability issues arising from autonomous AI in healthcare, noting that as AI shifts from assistive to independent decision-making, traditional malpractice and product liability laws must adapt. It calls for collaboration between legislators and the FDA to set clear standards based on AI autonomy, with strong oversight, quality control, and adherence to ethical principles like transparency, patient rights, and safety. The paper urges proactive laws to balance innovation with accountability and prevent legal ambiguities.

**Limitation or the research gap of the paper:** The referenced paper primarily examines civil liability frameworks such as medical malpractice and product liability within a U.S.-centric context, focusing on regulatory, ethical, and procedural issues around AI-driven

medical devices, but it does not address criminal liability. Key gaps relative to your research include the absence of analysis on criminal negligence, misconduct, and sanctions; lack of discussion on how Indian criminal law (IPC, CrPC) could apply; omission of enforcement mechanisms; limited consideration of Indian ethical, cultural, and legal contexts; and no adaptation to India's specific regulatory landscape. This leaves a substantial gap in exploring how criminal liability for medical robotics should be addressed within the Indian legal system.

## 7. Introduction

'The rapid integration of robotics and artificial intelligence into the medical domain marks a paradigm shift in contemporary healthcare delivery. 'Surgical robots, autonomous diagnostic systems, and AI-assisted therapeutic tools now augment, and in some instances substitute, human clinical judgment, promising enhanced precision, reduced human error, and improved patient outcomes'.[1] However, as robotic medical systems acquire increasing levels of decision-making autonomy, complex legal and ethical questions arise concerning accountability when such systems contribute to patient harm.[2] 'Traditional criminal law doctrine, rooted in human agency, intention, and fault, was not architected to govern autonomous systems capable of independent data-driven decisions.'[3] Consequently, the application of foundational elements such as mens rea, actus reus, negligence, and professional standards of care encounters doctrinal strain when confronted with machine action.

'India currently lacks a comprehensive legal framework addressing the criminal liability of medical robotics, relying instead on general provisions of healthcare regulation, product liability, and the criminal law framework under the Bharatiya Nyaya Sanhita (BNS) and associated regulatory statutes.' Unlike jurisdictions such as the European Union and the United States, where proactive legislative and ethical guidelines on autonomous systems have begun to emerge, India remains in an embryonic stage of legal preparedness.[4] 'This legislative lacuna raises pressing questions regarding culpability: whether liability should attach to surgeons supervising robotic procedures, manufacturers developing hardware, programmers engineering

[1] Satyanarayana R. and Manupati V.K., *AI-Assisted Surgery and Robotics: Impact on Healthcare Outcomes*, Journal of Medical Systems (2022).
[2] Calo R., *Robotics and the Lessons of Cyberlaw*, 103 Cal. L. Rev. (2015).
[3] Balkin J.M., *The Path of Robotics Law*, Yale Law School Research Paper No. 607 (2015).
[4] European Union, EU Artificial Intelligence Act (2024).

software algorithms, or healthcare institutions deploying such technology.'[5]

This research investigates these unresolved doctrinal dilemmas by critically analysing the adaptability of existing criminal law principles to autonomous medical systems, identifying regulatory deficiencies, and drawing comparative insights from global legal developments. The ultimate objective is to propose a structured criminal liability framework tailored to the Indian healthcare ecosystem, one that ensures patient safety, legal certainty, and technological innovation, without stifling the transformative potential of surgical and medical robotics.

## 8. Evolution of Medical Robotics: Global & Indian Context

'The evolution of medical robotics represents one of the most significant technological transformations in modern healthcare. The earliest phase of robotic integration in medicine centred around tele-operated systems designed to enhance surgical precision and enable remote assistance.'[6] First-generation platforms relied primarily on surgeon-controlled interfaces, where the robot functioned as an extension of the surgeon's skill rather than an independent medical actor. 'These developments emerged from military-funded tele-surgery initiatives and research into minimally invasive surgical support technologies, establishing foundational concepts such as motion scaling, tremor reduction, and enhanced visualisation.'[7]

'The second developmental phase witnessed the introduction of sophisticated robotic-assisted surgical systems capable of executing highly complex procedures with substantial improvements in accuracy and dexterity. Landmark innovations in this period include robotic applications in urology, cardiothoracic surgery, gynaecology, and oncology, where clinical outcomes demonstrated reduced blood loss, shorter hospital stays, and improved recovery times.'[8] As machine learning and advanced imaging systems matured, the role of robotics expanded beyond support functions into partial decision-making, particularly in preoperative planning, anatomical mapping, and intraoperative guidance.[9]

Contemporary research and industrial development mark a transition from assistive robotics to semi-autonomous and emerging autonomous platforms.[10] These systems increasingly

[5] Lodaya A., *Regulating Medical Robotics in India: Challenges & Prospects*, NUJS Law Review (2023).
[6] Taylor R.H., et al., *Medical Robotics and Computer-Integrated Surgery*, Springer (2016).
[7] Satava R.M., *Historical Development of Surgical Robotics*, Surgical Endoscopy (2003).
[8] Menon M., et al., *Robotic Surgery in Urology: Progress & Outcomes*, The Lancet (2020).
[9] Yang G.Z., et al., *Medical Robotics — A Review*, Science Robotics (2018).
[10] IEEE Robotics Standards Association, *Safety Standards for AI-Driven Robotic Surgery* (2021).

incorporate algorithmic decision-support tools, real-time data interpretation, and adaptive learning frameworks that enable the robot to refine movements, optimise surgical pathways, and respond dynamically to intraoperative variables. Such autonomy signals a shift from robotics as passive instruments to active agents participating in medical judgment and execution, thereby raising profound legal, ethical, and patient-safety considerations.[11]

India's integration of medical robotics has accelerated over the past decade, with leading tertiary-care institutions and corporate hospital networks adopting robotic surgical programs across varied specialities.[12] Major metropolitan centres have become hubs for robotic-assisted procedures, supported by partnerships between medical institutions, global robotics manufacturers, and domestic technology firms. Training modules, fellowships, and skill-development programs in robotic surgery have expanded rapidly in India, reflecting the medical profession's growing confidence in robotic interventions and patient demand for technologically advanced healthcare.[13]

Despite these advancements, concerns persist regarding reliability, high costs, inequitable access, and accountability for adverse outcomes.[14] Emerging scholarship in India highlights the tension between clinical benefits and legal uncertainty, particularly where complications arise in procedures involving automated functions or AI-driven surgical recommendations. While proponents emphasize enhanced precision, reduced error margins, and improved patient satisfaction, critics caution that increasing autonomy introduces risks of system malfunction, algorithmic error, and unclear chains of responsibility in the event of harm.[15]

Thus, the progression of medical robotics from tele-operated devices to autonomous surgical intelligence has ushered in unprecedented potential alongside new categories of legal and ethical obligations. The Indian context, characterised by rapid adoption but limited regulatory preparedness, underscores the urgency of establishing a structured liability and safety framework before robotic autonomy becomes a routine clinical reality.[16]

[11] United States FDA, Regulatory Framework for Surgical Robotics (2021).
[12] Apollo Hospitals, Annual Robotic Surgery Report (2023).
[13] Fortis Healthcare, Robotics Training & Clinical Integration Whitepaper (2022).
[14] NITI Aayog, *AI for All: Healthcare Deployment Report* (2021).
[15] Kumar D., *Legal Concerns in Autonomous Medical Robotics in India*, Indian Journal of Law & Technology (2022).
[16] World Health Organisation (WHO), *AI in Healthcare Governance Guidelines* (2023).

## 9. Theoretical Legal Framework Of Criminal Liability

### 9.1 Mens Rea & Actus Reus in Criminal Law

#### Traditional Foundations in Medical Negligence

'The concepts of actus reus (the wrongdoing) and mens rea (the guilty mind) have long served as the foundation for criminal liability in medical contexts.[17] In most medical negligence cases, a surgeon is held accountable for their failure to fulfil their duty, which results in harm to a patient.[18] This is typically assessed using the level of care that one would anticipate from a medical practitioner of reasonable skill. Therefore, proving that a medical professional's actions were wilfully harmful, egregiously negligent, or reckless is necessary to establish medical criminal liability. Courts have long acknowledged that physicians have a greater professional obligation because of their knowledge and authority over patient care, which entails a moral and legal obligation to safeguard life and health.'[19]

#### Challenges in Applying Mens Rea & Actus Reus to Medical Robotics

This conventional framework is complicated by the use of robotics and semi-autonomous systems in surgery.[20] The question of accountability arises when a robotic system moves or modifies its movements on its own.[21] It becomes difficult to identify the human agent responsible for the harm if it results from a mechanical failure or an algorithmic decision made by a machine. Furthermore, when autonomous systems lack consciousness, intent, or understanding, it becomes difficult to establish mens rea.[22]

A surgeon supervising a robotic procedure, for instance, might not have direct control over every movement.[23] The link between human intention and the act is weakened as a result.

---

[17] D.R. Mahmood et al., *Fixing Criminal Liability as per Elements of a Crime: A Review in Modern Era of AI and Robotics* (2023) Bahria University.
[18] Vikrant Yadav, *Robotics in Health Care: Who is Liable?* (2018) SSRN Electronic Journal https://doi.org/10.2139/ssrn.3598028.
[19] Massimo Farina & Alessia Palladino, *Medical Liability Issues (and Beyond) Resulting from the Use of New Technologies* in *New Technologies in Medical Practice* (Springer 2023).
[20] R.M.A. Razek, *Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges* (2024) 12(1) J. Law & Sustainable Development e2443.
[21] Fatima Al-Misbah, *The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability* (2024) 3 Int'l J. Sci. Research 91.
[22] Gabriel Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Boston 2020).
[23] Tamer Hamed Al-Qadi et al., *Risks of Artificial Intelligence in the Medical Field and Its Legal Implications* (2025) ResearchGate Publication 393253726.

Furthermore, software bugs, incorrect data interpretation, system delays, or deviations from machine learning can occasionally cause high-precision robotic actions to go wrong.[24]

### 9.2 Corporate & Vicarious Liability

#### Liability of the Surgeon / Medical Practitioner

Despite technological advancements, surgeons continue to be the primary clinical decision-makers and are required to provide continuous supervision during procedures involving robot assistance.[25] Therefore, the practitioner may be held accountable if harm results from inadequate supervision, inadequate training, inaction, or reckless reliance on automated systems. Whether a reasonably skilled surgeon using due diligence would have recognised the possible error and taken action to avoid it is the crucial question.[26] The direct liability of surgeons may, however, logically decline as robotic systems grow more autonomous, necessitating adjustments to reflect shared decision-making between humans and machines.[27]

#### Hospital / Institutional Liability

The safe and effective application of robotic technology is the responsibility of hospitals.[28] This entails providing appropriate instruction, keeping up with equipment maintenance, keeping an eye on operational standards, and putting patient safety procedures into practice. Failures in supervision systems, maintenance plans, or training programs can result in institutional neglect.[29] Furthermore, if hospital staff members cause harm while performing robot-assisted procedures, vicarious liability might be applicable. Therefore, hospitals are essential to the accountability process as both technology users and beneficiaries.[30]

#### Manufacturer and Software Programmer Liability

In conversations concerning medical liability, manufacturers and programmers are playing a bigger role, particularly when injuries are caused by poor system testing, unpredictable

[24] Julie E. Cohen, *The Right to Contest AI* (2021) 121 Columbia L. Rev. 1957.
[25] Erika Sophia Grossbard, *The AI-Robotic Prescription: Legal Liability When an Autonomous AI Robot is Your Medical Provider* (2023) 33 U. Miami Bus. L. Rev. 273.
[26] *Bharatiya Nyaya Sanhita*, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec. 2023).
[27] *Consumer Protection Act*, No. 35 of 2019 (India).
[28] *Information Technology Act*, No. 21 of 2000 (India).
[29] NITI Aayog, *Responsible AI for All: 2021 Strategy* (Government of India, 2021).
[30] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.

algorithms, programming errors, or design flaws.[31] Robotic surgical systems, in contrast to conventional medical instruments, have sophisticated software-driven decision-making and artificial intelligence that can independently process and modify data.[32] This calls into question product liability, negligent development practices, failure to warn, and accountability for the absence of protections against predictable harm. Manufacturers have a responsibility that extends beyond delivery and includes long-term behaviour monitoring, updates, and supervision as systems develop to employ machine learning and real-time adaptation.[33]

**Relevant Indian Legal Provisions**

There isn't currently a specific legal framework in Indian law for figuring out criminal liability related to autonomous medical systems. Rather, general statutory and common-law principles must be used to construct liability.[34] Basic criminal responsibility standards for carelessness and wrongdoing are outlined in the Bharatiya Nyaya Sanhita.[35] Product and service liability is covered by the Consumer Protection Act,[36] and regulations pertaining to cybersecurity and technology-related harm are covered by the Information Technology Act. Professional liability and duty-of-care standards are also influenced by established medical law.[37] Nevertheless, none of these frameworks specifically address algorithm-driven medical actions or autonomous decision-making, which creates legal ambiguity and practical enforcement problems.[38] A specific legislative and regulatory framework is required to address shared responsibility in cases of robotic medical harm, as this lack of legal clarity makes clear.[39]

## 10. Liability & Challenges in Robotic–Assisted Medical Harm

### 10.1 Duty of Care & Standard of Care

#### 1. Human Oversight Versus Robotic Autonomy

The traditional understanding of medical duty is altered by the introduction of robotics into

[31] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO Report, 2021).
[32] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).
[33] State of Maharashtra v. Hindustan Construction Co. Ltd., (2010) 4 SCC 518.
[34] D. Sayyed, *Artificial Intelligence and Criminal Liability in India* (2024) Cognitive Science Journal.
[35] *Bharatiya Nyaya Sanhita*, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec. 2023).
[36] *Consumer Protection Act*, No. 35 of 2019 (India).
[37] European Commission, *Proposal for an Artificial Intelligence Act* (COM/2021/206 final).
[38] Evalyn I. George et al., *Origins of Robotic Surgery: From Skepticism to Standard of Care* (2018) 22(4) JSLS e2018.00039.
[39] NITI Aayog, *Responsible AI for All: 2021 Strategy* (Government of India, 2021).

surgery.[40] Accountability is guaranteed because a surgeon typically has direct control over each stage of an operation.[41] The surgeon assumes a supervisory role during robotic and semi-autonomous procedures, while the robot performs designated tasks. This shift in control complicates how we assess the standard of care.[42] If a machine completes a task without human input, can a surgeon still be held accountable? When robotic systems employ adaptive algorithms or real-time data, the problem gets worse. Once closely associated with human hands, the duty of care now encompasses a complex technological environment. This calls into question what constitutes reasonable medical practice.[43]

### 2. Product Defect Versus Operator Negligence

Making the distinction between human error and machine failure is a frequent legal problem.[44] When complications occur, it can be challenging to determine whether the problem was caused by the robot or by the surgeon's error.[45] Inaccurate calibration, inadequate system training, inadequate planning, or misuse of robotic components can all lead to errors.[46] However, malfunctions may be brought on by software problems, sensor mistakes, or a loss of accuracy. Courts might incorrectly place blame if there are no clear rules or standards for robotic surgery.[47] This might result in unjust immunity for tech developers or unfair punishment for medical professionals. The case necessitates specific investigation techniques and legal clarity.[48]

## 10.2 Mens Rea Attribution to Autonomous Systems

### 1. Can a Robot Form Intent?

Human cognition—intent, foresight, and recklessness—is the foundation of criminal law.[49]

[40] Vikrant Yadav, *Robotics in Health Care: Who is Liable?* (2018) SSRN Electronic Journal https://doi.org/10.2139/ssrn.3598028.
[41] Evalyn I. George et al., *Origins of Robotic Surgery: From Skepticism to Standard of Care* (2018) 22(4) JSLS e2018.00039.
[42] Massimo Farina & Alessia Palladino, *Medical Liability Issues (and Beyond) Resulting from the Use of New Technologies* (Springer 2023).
[43] Tamer Hamed Al-Qadi et al., *Risks of Artificial Intelligence in the Medical Field and Its Legal Implications* (2025) ResearchGate Publication 393253726.
[44] Fatima Al-Misbah, *The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability* (2024) 3 Int'l J. Sci. Research 91.
[45] Fatima Al-Misbah, *The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability* (2024) 3 Int'l J. Sci. Research 91.
[46] Patrick Bolder, Michel Rademaker & Bianca Torossian, *Robotic and Autonomous Systems in a Military Context: The Future is Now, Prepare for 2045* (Hague Centre for Strategic Studies 2021).
[47] *Indian Medical Association v. V.P. Shantha*, (1995) 6 SCC 651.
[48] *Bharatiya Nyaya Sanhita*, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec 2023).
[49] *Consumer Protection Act*, No. 35 of 2019 (India).

Autonomous surgical robots, no matter how sophisticated, lack consciousness and morality.[50] Therefore, under the current system, assigning intent to machines is not legally valid. Whether human stakeholders exercised adequate oversight and caution is the true question. Traditional measures of intent are called into question as robotic independence increases; design, programming, monitoring, and operation errors can be the cause of negligence rather than a single actor. In this context, criminal liability may lessen unless the law adapts to include various technological inputs.[51]

### 2. Algorithmic Error Versus Human Error

AI-enabled robots can learn from data or adapt to changing conditions during surgery, unlike traditional tools.[52] An algorithm may produce erroneous movement paths, misidentify tissue, or misunderstand the dynamics of the surgical site.[53] These algorithmic mistakes are neither deliberate nor typically careless.[54] They draw attention to machine learning's shortcomings. However, human error results from poor decision-making, insufficient supervision, or improper system management.[55] Careful algorithm audits, training materials, system logs, and expert evaluations are necessary to comprehend these variations; these resources are not yet completely developed in India's legal system. When determining liability, a future legal system must take into account how algorithms behave and how machine-driven decisions vary.[56]

## 10.3 Chain of Responsibility

### 1. Surgeon

Clinical responsibility starts with the surgeon. Regardless of the level of robotic assistance, a healthcare provider must determine the patient's suitability, oversee the process, and step in when necessary.[57] If a surgeon depends too much on the robot or does nothing when there are obvious dangers, they could be held criminally liable. However, when surgeons operate within system limitations or when unexpected software behaviours occur, it is unreasonable to expect

[50] Information Technology Act, No. 21 of 2000 (India).
[51] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[52] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO Report, 2021).
[53] D. Sayyed, *Artificial Intelligence and Criminal Liability in India* (2024) Cognitive Science Journal.
[54] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).
[55] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.
[56] R.M.A. Razek, *Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges* (2024) 12(1) J. Law & Sustainable Development e2443.
[57] Gabriel Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Boston 2020).

them to be fully liable.[58]

**2. Hospital / Healthcare Institution**

Hospitals facilitate technology and are thus responsible for ensuring proper training, maintaining equipment, creating safe environments, and managing consent processes.[59] Institutional liability may come from poor system choices, inadequate training, lack of maintenance, or failure to carry out safety checks. Hospitals serve as the structural caretakers of robotic surgical systems.[60]

**3. Hardware Manufacturer**

It is the responsibility of manufacturers to develop dependable systems that are error-resistant and incorporate safety features, failure alerts, and testing procedures.[61] They are accountable for hardware problems such as malfunctioning sensors, actuators, or mechanical issues. The concepts of criminal negligence and product liability may be applicable if harm results from defects in the design or inadequate testing prior to market release.[62]

**4. Software / AI Developer**

The robot's decision-making and operation are shaped by machine-learning engineers and software developers. The developer's involvement becomes essential in determining liability if programming errors, biassed data, antiquated systems, or flawed algorithms cause harm.[63] In adaptive AI systems, accountability may go beyond the original design to encompass ongoing algorithmic monitoring, updates, and ethical standards. However, current legislation is vague about the point at which programmers become criminally liable.[64]

[58] Fatima Al-Misbah, *The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability* (2024) 3 Int'l J. Sci. Research 91.
[59] Haider Kazem Hathout, *Criminal Protection of Public Relations Related to Robots: A Comparative Study* (2024) 19(1) Int'l J. Criminal Justice Sciences 1.
[60] Evalyn I. George et al., *Origins of Robotic Surgery: From Skepticism to Standard of Care* (2018) 22(4) JSLS e2018.00039.
[61] *Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1.
[62] *Bharatiya Nyaya Sanhita*, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec 2023).
[63] D. Sayyed, *Artificial Intelligence and Criminal Liability in India* (2024) Cognitive Science Journal.
[64] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).

## 11. Comparative International Legal Analysis

Major legal systems around the world have been forced to reconsider conventional notions of liability, patient safety, and regulatory responsibility as a result of technological advancements in medical robotics.[65] Although no jurisdiction has developed an ideal legal framework for autonomous surgical systems, each has its own distinct methods that expose different regulatory philosophies and tactics.[66] Three different models are revealed by a detailed comparison of the US, UK, and EU: the US has a market-driven and litigation-guided approach, the UK has a patient-safety and governance framework, and the EU has a precaution-driven regulatory system.[67] When combined, these models can offer valuable insights for India, which is currently governed by general criminal and consumer protection laws and lacks a clear liability system for medical robotics.[68]

### 11.1 European Union: Risk-Based Regulation and Evolving Liability Standards

The precautionary, risk-based regulatory philosophy that underpins the European approach seeks to strike a balance between safety requirements and unambiguous accountability. This regulatory framework's primary goals are to categorise AI-driven systems according to their degree of risk and to place stringent requirements on high-risk applications, like medical robotics.[69] Strong pre-market evaluations, thorough documentation to guarantee traceability, explainability requirements whenever feasible, and continuing monitoring following market introduction to detect and address new harms are typical examples of these responsibilities.[70]

At the same time, the EU is demonstrating interest in revising its liability regulations to ensure that victims of harm caused by algorithm-driven or autonomous systems have access to sufficient remedies.[71] This involves taking into account modifications to stringent and fault-based liability laws that would enable plaintiffs to avoid demonstrating personal human fault in cases where harm results from intricate socio-technical systems. Mandatory safety features, increased producer responsibility, and more precise evidence standards are suggested by the

[65] European Commission, *Proposal for an Artificial Intelligence Act* (COM/2021/206 final).
[66] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.
[67] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[68] NITI Aayog, *Responsible AI for All: 2021 Strategy* (Government of India, 2021).
[69] R.M.A. Razek, *Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges* (2024) 12(1) J. Law & Sustainable Development e2443.
[70] Tamer Hamed Al-Qadi et al., Risks of Artificial Intelligence in the Medical Field and Its Legal Implications (2025).
[71] Gabriel Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Boston 2020).

proposed reforms (e.g., shifting the burden to operators or producers to show due care if the system lacks transparency).[72]

The advantages of (a) a risk-based regulatory framework that automatically identifies medical robotics as high-risk, (b) mandatory technical and procedural requirements (such as testing, explainability, and logging), and (c) liability measures that reduce the burden of proof on victims when the cause of harm is complex are all illustrated by the EU model for India.[73] Safety and accountability function best when technical responsibilities and legal remedies complement one another, as demonstrated by the EU's combined regulatory and liability approach.[74]

### 11.2 United States: Regulatory Oversight, Case-Based Liability, and Market-Driven Controls

In order to regulate medical devices, including software and robotic systems, the US employs a more decentralised regulatory model, depending on specialised organisations, particularly the Food and Drug Administration. While tort law (product liability and medical malpractice) has a significant influence on clinical operations and manufacturer practices, the regulatory focus is on pre-market approval processes, risk classification, and post-market monitoring.[75]

Liability develops through individual cases, as demonstrated by U.K. legal practices. Medical malpractice claims target healthcare providers for improper use or lack of supervision, while product liability claims are typically filed against manufacturers for design, manufacturing, or warning defects.[76] These cases frequently involve a great deal of technical analysis and expert testimony. As part of compliance strategies, the market-driven environment also encourages stringent quality systems, comprehensive documentation, and industry-led standards.[77] However, relying solely on tort law can put plaintiffs under a lot of strain, particularly when dealing with proprietary or ambiguous algorithms, making it challenging to prove fault and

[72] Patrick Bolder, Michel Rademaker & Bianca Torossian, *Robotic and Autonomous Systems in a Military Context: The Future is Now, Prepare for 2045* (Hague Centre for Strategic Studies 2021).
[73] Julie E. Cohen, *The Right to Contest AI* (2021) 121 Columbia L. Rev. 1957.
[74] Erika Sophia Grossbard, *The AI-Robotic Prescription: Legal Liability When an Autonomous AI Robot is Your Medical Provider* (2023) 33 U. Miami Bus. L. Rev. 273.
[75] U.S. Food and Drug Administration (FDA), *Artificial Intelligence and Machine Learning in Medical Devices: Guidance for Industry and FDA Staff* (2023).
[76] UK Department of Health & Social Care, *Medical Devices Regulations and Patient Safety Framework* (2022).
[77]UK Parliament, *Health and Care Act*, 2022 (UK).

causation.

The United Kingdom combines statutory and institutional methods, focusing on patient safety standards, clinical governance, and professional accountability. Healthcare institutions, particularly the National Health Service (NHS), create and enforce clinical guidelines for the safe use of technologies. This includes structured training programs, credentialing requirements for operators, and specific operating protocols for each system. The UK approach emphasizes institutional readiness, ensuring hospitals have the governance structures, audit mechanisms, and incident review processes needed to safely incorporate robotics

### 11.3 United Kingdom: Integrated Patient-Safety Focus and Institutional Protocols

In the UK, professional accountability, clinical governance, and patient safety standards are prioritised through a combination of institutional and statutory approaches.[78] Clinical guidelines for the safe use of technologies are developed and enforced by healthcare organisations, especially the National Health Service (NHS). This includes structured training programs, credentialing requirements for operators, and specific operating protocols for each system.[79] The UK strategy places a strong emphasis on institutional preparedness, making sure hospitals have the auditing, governance, and incident review systems necessary to safely integrate robotics.[80]

The significance of open reporting, root-cause analysis, and incident learning is also emphasised by UK regulatory and patient safety systems. The system frequently favours investigative responses that distinguish between human error, system flaws, and unpredictable algorithm behaviour rather than hastening criminalisation. For instances of egregious carelessness or wilful disregard, the criminal justice system is still accessible and can hold people or institutions accountable when needed.

The UK model highlights the significance of incorporating technology adoption into the country's current institutional frameworks for India.[81] This includes establishing standards by

[78] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO Report, 2021).
[79] Haider Kazem Hathout, *Criminal Protection of Public Relations Related to Robots: A Comparative Study* (2024) 19(1) Int'l J. Criminal Justice Sciences 1.
[80] Fatima Al-Misbah, *The Legal Personality of Robotic Surgery and the Possibility of Determining Criminal Liability* (2024) 3 Int'l J. Sci. Research 91.
[81] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).

healthcare providers, requiring operator credentialing, putting in place a systematic incident reporting and analysis process, and making sure that, when appropriate, enforcement strikes a balance between education and punishment.[82]

### 11.4 Comparative Synthesis: Lessons for India

The comparative analysis identifies complementary strengths among jurisdictions, including the UK's institutional patient-safety protocols and calibrated investigatory culture; the U.S. focus on technical regulator capacity and tort remedies; and the EU's comprehensive risk-regulatory architecture and liability modernisation. Instead of adopting a single transplanted model, these lessons recommend a multifaceted approach for India. Important lessons learnt include:[83]

- Treat medical robotics as inherently high-risk and subject them to enhanced pre-market and post-market controls.[84]
- Mandate robust technical documentation, logging, and explainability where feasible to facilitate forensic investigation.[85]
- Strengthen a specialised regulatory authority for medical devices and AI with investigatory and incident-reporting powers.[86]
- Adapt liability doctrines to account for algorithmic causation—through evidentiary presumptions, producer obligations, and statutory clarification—so victims are not left without remedy due to technical opacity.[87]
- Institutionalise mandatory training, credentialing, and governance protocols within hospitals to ensure safe deployment and clear chains of responsibility.[88]

When combined, these steps can assist India in developing a cogent legal and policy response that maintains the therapeutic advantages of robotic innovation while offering strong

[82] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.
[83] UK Department of Health & Social Care, supra note 17.
[84] Cohen, supra note 11.
[85] Grossbard, supra note 12.
[86] Al-Qadi, supra note 7.
[87] Farina & Palladino, supra note 6.
[88] Yadav, supra note 9.

accountability in the event that technology malfunctions.

## 12. Indian Legal Landscape & Identified Gaps

Aspects of technology-driven medical practice are currently addressed by the Indian legal system through a number of laws, rules, and professional standards.[89] Nevertheless, this disjointed strategy fails to foresee or adequately address the particular difficulties presented by autonomous medical robotics.[90] Regarding criminal liability for harm caused by robots, the following analysis examines important laws and finds gaps in doctrine, evidence, institutions, and policies.[91]

### 12.1 Existing Statutory and Regulatory Instruments

India's approach to healthcare technology is multi-layered and dispersed throughout different legislative and administrative frameworks.[92] The Bharatiya Nyaya Sanhita (BNS) establishes the boundaries of criminal responsibility for human actors and offers the framework for criminal law with regard to carelessness, injury, and death brought on by wrongdoing.[93] Patients injured by medical devices or institutional failures can seek civil remedies under the Consumer Protection Act, which addresses faulty goods and subpar services.[94] A legal framework for online safety and computer-related offences is provided by the Information Technology Act, which addresses digital systems, cybersecurity, and electronic records. While the Telemedicine Guidelines convert forward-looking policies into practice standards for remote healthcare, the Medical Device Rules and associated regulations guarantee pre-market approval, safety standards, and post-market monitoring of medical devices.[95]

Collectively, these laws govern various aspects of the medical robotics ecosystem, such as digital integrity, device safety, consumer rights, criminal responsibility, and clinical practice.[96] They do not, however, come up with a cohesive response to autonomous machines that

[89] Bharatiya Nyaya Sanhita, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec. 2023).
[90] Vikrant Yadav, *Robotics in Health Care: Who is Liable?* (2018) SSRN Electronic Journal.
[91] D.R. Mahmood et al., *Fixing Criminal Liability as per Elements of a Crime: A Review in Modern Era of AI and Robotics* (2023) Bahria University.
[92] Massimo Farina & Alessia Palladino, *Medical Liability Issues (and Beyond) Resulting from the Use of New Technologies* (Springer 2023)
[93] Consumer Protection Act, No. 35 of 2019 (India).
[94] Medical Device Rules, 2017, Ministry of Health and Family Welfare, Government of India.
[95] Telemedicine Practice Guidelines, 2020, Board of Governors in supersession of Medical Council of India.
[96] Tamer Hamed Al-Qadi et al., *Risks of Artificial Intelligence in the Medical Field and Its Legal Implications* (2025).

integrate data training, hardware, software, real-time adaptation, and continuous learning. Gaps in coordination and coverage become more noticeable as robotics progresses from assistive tools to semi-autonomous clinical agents.[97]

### 12.2 Doctrinal and Evidentiary Gaps

Applying current criminal law concepts to harm caused by robotics presents significant doctrinal challenges. Human intent is the foundation of the BNS and associated laws. A human agent with the capacity for knowledge, intention, or recklessness is implied by mens rea and actus reus. Since autonomous algorithms are not sentient and cannot have mens rea, it is difficult to directly attribute criminal responsibility to them.[98] Whether to (a) expand on current mens rea concepts by indirectly attributing intent or knowledge to humans, (b) examine new models of strict liability for risky autonomous activities, or (c) develop hybrid doctrines to capture shared blame between humans and organisations would be the decision that courts dealing with robotic-related harm would need to make.[99]

Evidentiary challenges exacerbate these doctrinal issues.[100] Algorithmic decision-making, which necessitates specialised technical knowledge, frequently involves large machine logs and opaque, proprietary models.[101] Without legal guidelines for logging, auditing, and disclosure, victims and courts are left with a significant information gap.[102] To prove causation—that is, that a specific algorithmic action, sensor malfunction, or software update caused harm—forensic expertise, source code access, and thorough documentation are required. The technical procedures necessary for post-event analysis, as well as explicit regulations mandating mandatory disclosure from manufacturers and data controllers, are absent from the current legal framework.[103]

### 12.3 Institutional and Regulatory Fragmentation

Medical robotics is governed by a number of agencies and regulatory bodies. Device approvals

[97] R.M.A. Razek, *Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges* (2024) 12(1) J. Law & Sustainable Development e2443.
[98] Kusum Sharma & Ors. v. Batra Hospital & Medical Research Centre & Ors., (2010) 3 SCC 480.
[99] Indian Medical Association v. V.P. Shantha, (1995) 6 SCC 651.
[100] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[101] NITI Aayog, *Responsible AI for All: 2021 Strategy* (Government of India, 2021).
[102] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.
[103] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO Report, 2021).

are overseen by health regulators. Cybersecurity is supervised by information technology authorities. While the criminal justice system handles prosecutions, consumer forums handle product disputes. Confusion regarding enforcement, evidentiary standards, and investigative authority results from this fragmentation.[104] Responses to incidents could be sluggish, uneven, or lacking in a coordinated inter-agency approach or a lead regulator. Furthermore, disparate state-level healthcare laws may lead to disparate enforcement practices, resulting in a regulatory "patchwork" that compromises uniform accountability.[105]

### 12.4 Standards of Care, Clinical Governance, and Professional Accountability

According to recognised clinical protocols, peer practice comparisons, and professional competence, Indian medical law evaluates negligence. Nevertheless, there are no particular safety guidelines for algorithm-assisted or robotic procedures.[106] There are still important questions regarding the education and certification required for surgeons to operate robotic systems, the degree of supervision required as autonomy rises, and how informed consent should change to account for algorithmic decision-making and the risks involved. Courts may find it difficult to apply analogical reasoning that takes into account the technical realities of robotic systems in the absence of explicit institutional protocols and required credentials.[107]

### 12.5 Corporate Liability and Manufacturer Obligations

Indian law lacks explicit obligations pertaining to technology, even though corporate vicarious liability permits organisations to be held accountable for the acts of their agents. It is not necessary for software developers and manufacturers to continuously monitor algorithms, put important safety precautions in place, or maintain thorough logs for forensic purposes.[108] Criminal liability is still unclear and underdeveloped; the Consumer Protection Act only addresses faulty goods and services and provides civil remedies. There are no explicit legal penalties for neglecting to address known algorithmic risks, nor is there a duty to continuously monitor algorithms that change after deployment.[109]

---

[104] Patrick Bolder, Michel Rademaker & Bianca Torossian, *Robotic and Autonomous Systems in a Military Context: The Future is Now, Prepare for 2045* (Hague Centre for Strategic Studies 2021).
[105] D. Sayyed, *Artificial Intelligence and Criminal Liability in India* (2024) Cognitive Science Journal.
[106] Press Information Bureau, Government of India, *Medical Robotics Adoption in India: Challenges and Roadmap* (2024).
[107] WHO & OECD, *AI Readiness Assessment for Health Systems* (2022).
[108] Ministry of Electronics and IT (MeitY), *AI Governance Framework for India* (2024).
[109] OECD, *Artificial Intelligence in Healthcare: Opportunities and Challenges* (2021).

### 12.6 Data Protection, Privacy, and Procedural Rights

Data handlers, such as healthcare providers and device manufacturers, are subject to obligations under India's data protection laws, which primarily address privacy, consent, and penalties for violations. Criminal liability for bodily harm brought on by algorithmic decisions is not established by these laws.[110] The relationship between machine accountability and medical data governance is still evolving; for instance, it is still unclear if biassed clinical judgements resulting from inadequately trained datasets could result in criminal liability. Furthermore, current laws do not specifically grant patients the ability to contest algorithmic decisions, obtain system logs, or request independent audits.[111]

### 12.7 Practical and Capacity Constraints

Lastly, real-world challenges impede efficient enforcement. There is a lack of certified forensic labs that can analyse sophisticated machine-learning systems, and courts and prosecutors frequently lack the technical know-how to determine algorithmic causation. It's possible that regulatory agencies lack the resources, personnel, or legal power to demand disclosures from global manufacturers. These restrictions have an impact on accountability following harm as well as preventive regulation.[112]

### 12.8 Summary of Identified Gaps

1. Autonomous medical robotics lacks a defined criminal liability framework.

2. Inconsistency between machine autonomy and criminal law based on mens rea.

3. The lack of required logging/traceability and opaque algorithms result in gaps in the evidence.

4. The lack of a lead authority for medical robotics and fragmented regulations.

5. There are no particular clinical governance, credentialing, or standards of care for robotic

[110] World Economic Forum, *Global AI in Healthcare Governance Report* (2023).
[111] Internet and Mobile Association of India (IAMAI), *AI and Legal Liability in Indian Healthcare Sector* (2023).
[112] OECD, *Global Forum on AI Safety in Health Applications* (2023).

techniques.

6. Limited legal requirements for continuous monitoring, updates, and disclosures on the part of software developers and manufacturers.

7. Restricted patient rights to access investigative data or contest algorithmic decisions.

8. Problems with capacity and resources in judicial, regulatory, and forensic organisations.

### 12.9 Immediate Regulatory Needs (Indicative)

Legal requirements for technical logging and incident disclosures, mandatory certification and training for robotic operators, mandatory reporting of adverse events and the creation of a central incident registry, as well as the development of specialised technical forensic capabilities within regulatory or prosecutorial agencies, are some immediate steps that could greatly improve accountability, even though more detailed recommendations will be revealed later.[113] By putting these steps into place, the responsibility gap would be reduced and criminal investigations into robotic harm would become more practical.[114]

## 13. Proposed Legal Solutions & Reform Model

A thoughtful combination of precise legislation, technological protections, robust institutions, and efficient practices is required to establish a sound legal framework for criminal liability in medical robotics.[115] Together, these components ought to delegate accountability while preserving room for creativity.[116] The following suggestions are meant to be realistic, compliant with the law, and sensitive to the realities of autonomous and robot-assisted surgery.[117]

### 13.1 A Dedicated Statutory Framework

We require a distinct law, either as an independent "Medical Robotics Act" or as a component

[113] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).
[114] Ministry of Electronics and IT (MeitY), *AI Governance Framework for India* (2024).
[115] European Commission, *Proposal for an Artificial Intelligence Act* (COM/2021/206 final, 2021).
[116] OECD, *AI Principles: Recommendations on Artificial Intelligence* (2019) OECD Legal Instruments 0425.
[117] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health* (WHO Report, 2021).

of an updated health technology law.[118] This will assist us in overcoming the uneven application of current consumer and criminal laws. Important characteristics ought to consist of:

1. Clear Definitions: To avoid misunderstandings, important terms like medical robotics, autonomous system, semi-autonomous system, operator/supervising surgeon, manufacturer, software developer, and deployment institution should have statutory definitions.[119]

2. Classification of Autonomy: a tiered system that differentiates between assistive tools and surgical systems that are semi-autonomous or fully autonomous (e.g., Levels 0–4). Each level's risk should be matched by its legal obligations.[120]

3. Express Liability Norms: clauses outlining the circumstances in which criminal liability may be applicable. This covers (a) egregious human actor negligence (e.g., surgeons, supervisors); (b) corporate liability for careless actions or systemic failures; and (c) circumstances that give rise to strict or objective liability for autonomous high-risk operations.[121]

4. Burden-shifting Mechanisms: The statute may establish a rebuttable presumption if algorithmic opacity makes it difficult for victims to establish causation. This would transfer the onus of proof to the operator or producer to demonstrate compliance with safety, testing, and monitoring requirements.[122]

### 13.2 Liability Allocation Matrix

A legal framework should lay out standard allocations of responsibility while allowing for adjustments based on the situation. Core features:

1. Surgeon / Operator: primary responsibility for patient selection, supervision, real-time intervention, and ensuring valid informed consent that specifically addresses robotic or autonomous elements. Criminal liability applies only when gross negligence or reckless

[118] NITI Aayog, *Responsible AI for All: 2021 Strategy* (Government of India, 2021).
[119] Bharatiya Nyaya Sanhita, No. 45 of 2023, Gazette of India, Extraordinary, Part II, Section 1 (25 Dec. 2023).
[120] Vikrant Yadav, *Robotics in Health Care: Who is Liable?* (2018) SSRN Electronic Journal https://doi.org/10.2139/ssrn.3598028.
[121] R.M.A. Razek, *Criminal Responsibility for Errors Committed by Medical Robots: Legal and Ethical Challenges* (2024) 12(1) Journal of Law & Sustainable Development e2443.
[122] Gabriel Hallevy, *When Robots Kill: Artificial Intelligence Under Criminal Law* (Boston 2020).

disregard is proven.[123]

2. Hospital / Institution: must ensure the purchase of safe devices, establish credentialing and training programs, maintain maintenance and audit cycles, and ensure incident reporting. Vicarious liability can occur if there is systematic negligence or failure in governance.[124]

3. Manufacturer / Hardware Vendor: must meet strict obligations for design safety, physical reliability, maintenance instructions, and fail-safe hardware controls. Criminal liability arises when grossly negligent design or failure to provide safety information results in harm.[125]

4. Software/AI Developer: must remove known biases, follow strict update/rollback protocols, validate algorithms on representative datasets, and provide explainability logs. Wilful concealment of serious flaws or careless deployment without mitigation are criminally exposed.[126]

5. Shared/Hybrid Liability: When several factors contribute to a cause, liability should be divided based on the extent of each factor's contribution and contractual or legal obligations. Courts will benefit from statutory guidance on proportionality.[127]

Rules for determining joint liability, guidelines for assigning blame, and guidelines for sentencing or sanctioning corporate actors should all be included in the matrix.

### 13.3 Mandatory Safety Standards, Audit Trails, and Compliance Mechanisms

**Technical and procedural safeguards should be required and enforceable:**

1. Pre-market Conformance & Certification: stringent conformance evaluations for systems with a high degree of autonomy, encompassing human-override mechanisms, safety redundancies, and clinical validation.[128]

2. Post-market Surveillance and Incident Reporting: required, timely reporting of adverse

[123] *Jacob Mathew v. State of Punjab*, (2005) 6 SCC 1.
[124] Indian Medical Association v. V.P. Shantha, (1995) 6 SCC 651.
[125] Kusum Sharma & Ors. v. Batra Hospital & Medical Research Centre & Ors., (2010) 3 SCC 480.
[126] State of Maharashtra v. Hindustan Construction Co. Ltd., (2010) 4 SCC 518.
[127] US FDA, *Artificial Intelligence and Machine Learning in Medical Devices: Guidance for Industry and FDA Staff* (2023).
[128] ISO 13485:2016, *Medical Devices—Quality Management Systems—Requirements* (ISO, 2016).

events to a central registry, as well as summary reports made available to the public to inform patients and practitioners.[129]

3. Comprehensive Audit Logs: required by law to record operator commands, software versions, sensor readings, update histories, and decision-making processes. Logs must be preserved for a legally specified amount of time and be tamper-evident.[130]

4. Explainability & Documentation: Developers are required to supply materials that are appropriate for expert forensic analysis and clinical review, as well as clear documentation.[131]

5. Mandatory Insurance & Compensation Mechanisms: Organisations and manufacturers ought to have mandatory product liability and professional insurance, along with a fund to guarantee prompt victim compensation.[132]

### 13.4 Institutional Reform: Medical Robotics Regulatory Authority of India (MRRAI)

The Medical Robotics Regulatory Authority of India (MRRAI), a specialised regulator with statutory authority, ought to be established to supervise medical robotics throughout its whole lifecycle.[133]

**Roles and Capabilities:**

1. Give high-risk systems conformance certificates and pre-market approvals.

2. Keep the National Robotics Incident Registry up to date and require that major adverse events be reported right away.

3. Demand the release of system logs and source materials and order forensic audits (while respecting legitimate IP protections and confidentiality).

4. Establish legally binding guidelines for manufacturer supervision, hospital administration, and operator credentialing.

[129] Telemedicine Practice Guidelines, 2020, Board of Governors in supersession of Medical Council of India.
[130] Medical Device Rules, 2017, Ministry of Health and Family Welfare, Government of India.
[131] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[132] United Nations Interregional Crime and Justice Research Institute (UNICRI), *AI and Criminal Justice: Challenges and Opportunities* (2022).
[133] Julie E. Cohen, *The Right to Contest AI* (2021) 121 Columbia Law Review 1957.

5. Work with prosecutorial agencies, recommend criminal investigations in cases of egregious misconduct, and impose administrative penalties.

6. Work together globally on incident sharing and technical standards.

**Structure and Safeguards:**

1. Multi-disciplinary teams that include clinicians, legal experts, AI engineers, and patient representatives.

2. Procedural safeguards to protect trade secrets while ensuring access for investigations (e.g., protective orders, accredited forensic laboratories).

3. Open rule-making and consultations with stakeholders to maintain trust.

**13.5 Explainable and Accountable AI Systems**

As a fundamental requirement for compliance, legal requirements should guarantee accountability in algorithms:[134]

1. Design-for-Explainability: In order to reconstruct important choices that had a major influence on patient outcomes, developers must incorporate explainability features into their designs.

2. Continuous Validation: continuous validation against performance thresholds and clinical datasets; a mandatory rollback if performance deteriorates.

3. Bias Audits & Data Governance: impartial evaluations of the representativeness and fairness of datasets; documented strategies to rectify biases discovered.

4. Right to Contest & Access: Patients (or their designated representatives) must be able to contest algorithmic decisions that result in negative outcomes and obtain an easily readable summary of the reasoning and pertinent logs.

[134] European Commission, *Product Liability Directive (recast) Proposal* (COM/2022/495 final, 2022).

### 13.6 Procedural and Evidentiary Reforms

To facilitate the management of criminal proceedings:[135]

1. Forensic Frameworks: certification of specialised forensic laboratories for the analysis of algorithms and devices in accordance with predetermined guidelines.

2. Expert Panels: multidisciplinary panels established by statute to counsel courts on complex causality matters.

3. Disclosure Rules: legal guidelines that balance the interests of national security and intellectual property by requiring the disclosure of logs and diagnostic materials under court supervision.

4. Evidentiary Presumptions: presumptions that, for instance, shift the burden of demonstrating compliance to the producer or operator when unexplained system anomalies occur with incidents.

### 13.7 Transitional & Safeguard Measures

To strike a balance between accountability and innovation:[136]

1. Safe-Harbour for Compliance: organisations that blatantly adhere to MRRAI certification, reporting, and standards are shielded from harsh penalties for certain technical errors. This promotes obedience rather than secrecy.

2. Phased Implementation: regulations for the highest-risk systems should be prioritised, and lower-risk categories should be rolled out later.

3. Capacity Building: establish accredited training programs for hospital technologists and surgeons, enhance the technical proficiency of the regulatory body, and provide judicial training on AI and robotics.

[135] Parliamentary Standing Committee on S&T, *AI and Robotics in Public Health Sector Report* (2024).
[136] Internet and Mobile Association of India (IAMAI), *AI and Legal Liability in Indian Healthcare Sector* (2023).

### 13.8 International Cooperation and Standards Alignment

India should adopt compatible standards and engage in cross-border collaboration[137]:

1. To encourage trade and guarantee adherence to best practices, align MRRAI standards with internationally accepted benchmarks (ISO, IEC, and EU standards).

2. Create agreements for mutual aid in cross-border enquiries involving global vendors.

3. Establish data-sharing guidelines for early-warning and incident-learning systems.

### 13.9 Enforcement, Penalties, and Remedies

Criminal penalties should be appropriate and specific[138]:

1. Individual criminal liability is restricted to situations in which managers or practitioners have engaged in wilful misconduct, extreme carelessness, or recklessness.

2. Corporate criminal liability is applicable in cases where there is evidence of corporate culture, careless profit-making at the expense of safety, or deliberate concealment of flaws.

3. Administrative and Civil Remedies: The enforcement framework should be supplemented by administrative fines, mandatory corrective actions, and civil compensation.

4. Remedial Prioritisation: put more emphasis on restitution for victims, maintaining public safety, fixing problems, and enhancing systems than just punishing them.

### 13.10 A Balanced & Pragmatic Reform Package

By providing safe harbours for compliant entities and incremental implementation, the proposed reform model seeks to (a) clarify legal liability in medical robotics, (b) provide efficient investigative and evidentiary processes for determining causes and responsibilities, (c) align regulation with the technical realities of adaptive AI systems, and (d) promote an innovation-friendly environment. When taken as a whole, these actions can improve patient

[137] IEC 60601-1:2005+A1:2012, *Medical Electrical Equipment—Part 1: General Requirements for Basic Safety and Essential Performance* (International Electrotechnical Commission, 2012).
[138] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on Medical Devices (EU MDR) [2017] OJ L117/1.

safety, bridge the accountability gap, and place India among nations with comprehensive, cutting-edge medical robotics governance.[139]

## 14. Conclusion

The rapid adoption of artificial intelligence and robotics in medicine represents a significant shift in the way healthcare is provided. Through tele-robotics and autonomous systems, this technology promises less invasive procedures, more accurate surgeries, fewer mistakes, and wider access to specialised knowledge. But this change also calls into question long-standing legal precepts, particularly those pertaining to criminal liability and medical malpractice.[140] The study draws attention to a significant problem: India's current legal frameworks, which are founded on human-centered fault models and standard medical negligence principles, are ill-prepared to address the unique risks associated with shared responsibility, autonomous medical systems, ambiguous algorithms, and clinical judgements made by machines.[141]

The results show significant issues. First, determining criminal liability in situations involving robotic harm is challenging. This is because a number of people, including physicians, engineers, developers, hospitals, and self-governing algorithms, are involved. Second, when harm can arise from unanticipated machine actions that human operators cannot predict, biassed training data, software updates, or hidden algorithmic flaws, depending solely on conventional notions of mens rea is insufficient.[142] Third, the absence of clear regulations may expose medical professionals to irrational legal risks while enabling software developers and manufacturers to shield themselves from liability by citing technical issues. Fourth, a global trend towards algorithmic accountability and risk-classification systems can be seen when comparing major regions such as the EU, USA, and UK. This highlights how urgently India must implement coordinated.[143]

The urgency of the law is obvious. Lagged regulations may impede innovation and result in needless harm, evidence-related problems, and public mistrust of life-saving technologies, as evidenced by the growing use of robotic surgery in leading Indian hospitals and rising private

[139] Bureau of Indian Standards, IS/ISO 81001-1:2021, Health Software and Health IT Systems Safety—Part 1: Principles and Concepts (BIS, 2022 reprint).
[140] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[141] National Digital Health Blueprint (NDHB), *Ministry of Health & Family Welfare* (2019).
[142] 21 C.F.R. Part 803, *Medical Device Reporting (MDR)* (U.S.).
[143] Companies Act, 2013 (India), ss. 447–454 (offences, penalties, fraud, and liability of officers).

investments in medical AI platforms. The criminal justice system runs the risk of either punishing medical professionals excessively or failing to hold businesses and algorithm developers accountable in the absence of clear laws, which would increase the "responsibility gap" in tech-enhanced healthcare.[144]

In the future, legislators ought to concentrate on developing a specific legal framework for medical robotics that incorporates varying degrees of autonomy, explicit guidelines for roles, and specifications for algorithm audits. Certification, audit trails, data registries, and malpractice investigations should all be overseen by the proposed Medical Robotics Regulatory Authority of India (MRRAI).[145] To ensure equitable decision-making and preserve patient trust, it is critical to acknowledge the necessity of explainability, algorithmic transparency, and access to system logs. Additionally, ethical considerations like human oversight, equitable training data, privacy-focused designs, required informed consent for AI use, and development protocols focused on preventing harm must be incorporated into safeguards.[146]

In summary, proactive regulatory governance is needed in the field of medical robotics, replacing reactive legal models. It is imperative that a well-rounded framework that is based on responsibility, suitable criminal liability, patient protection, and innovation support be put into place.[147] Only by making such progressive adjustments will India be able to fully realise the revolutionary potential of medical robotics while upholding the constitutional principles of justice, safety, dignity, and equal access to cutting-edge healthcare.[148]

[144] OECD, Health Data Governance: Privacy, Monitoring and Security (OECD Publishing, 2019).
[145] G20 New Delhi Leaders' Declaration (9–10 September 2023), paras on digital public infrastructure and responsible AI.
[146] National Medical Commission (NMC), *Registered Medical Practitioner (Professional Conduct) Regulations* (2023).
[147] *Poonam Verma v. Ashwin Patel*, (1996) 4 SCC 332.
[148] Bharatiya Sakshya Adhiniyam, 2023 (India) [Evidence law replacement; evidentiary presumptions and digital records].