

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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

AI IN HEALTHCARE: LEGAL REGULATION OF AI-BASED DIAGNOSIS AND TREATMENT IN INDIA — A COMPARATIVE STUDY WITH THE EUROPEAN UNION AND THE UNITED STATES

AUTHORED BY - ARPIT MEENA, YUVRAJ SINGH DERWAL
& KAUSHAL KISHOR MEENA
National Law Institute University, Bhopal, Madhya Pradesh, India

Abstract

Artificial intelligence (AI) has moved from the margins of medicine to its working core. Algorithms now read radiological images, flag deteriorating patients, triage emergency cases and recommend treatment pathways, and regulators have authorised well over a thousand AI-enabled medical devices. Legal systems built around the individual clinician and the static medical device are strained by technologies that are opaque, that may change after deployment and that can fail systematically rather than accidentally. The central question is who bears legal responsibility when AI-assisted diagnosis or treatment injures a patient, and which regulatory architecture is best placed to prevent that injury.

This paper examines the legal regulation of AI-based diagnosis and treatment in India and compares it with the European Union and the United States. India has no AI-specific statute; the field is governed by the professional-negligence doctrine developed in *Jacob Mathew v State of Punjab* and *Indian Medical Association v VP Shantha*, the Consumer Protection Act 2019, the Medical Devices Rules 2017, the Telemedicine Practice Guidelines 2020, the ICMR ethical guidelines of 2023, the Digital Personal Data Protection Act 2023 and the CDSCO's draft guidance on medical device software of October 2025. The European Union has adopted a horizontal, risk-based statute in the AI Act, layered on the Medical Device Regulation, the General Data Protection Regulation and a revised Product Liability Directive, although the application dates for high-risk systems have recently been deferred. The United States regulates through device law administered by the Food and Drug Administration, a statutory carve-out for certain clinical decision support software, state tort law and an emerging body of state legislation. The paper draws on decisions including *Canterbury v Spence*, *Riegel v Medtronic*, *Taylor v Intuitive Surgical*, *Estate of Lokken v UnitedHealth Group*, *SCHUFA Holding (Scoring)* and *SNITEM and Philips France*.

It argues that India should neither wait for a comprehensive AI statute nor transplant a foreign model wholesale. Instead, it should adopt a calibrated, sector-specific framework that preserves the clinician's non-delegable professional duty, recognises an independent institutional duty on hospitals that procure and deploy clinical AI, extends product liability to software, and imposes transparency, logging, consent and bias-audit obligations proportionate to risk. The paper concludes by proposing legislative and regulatory reforms that allocate responsibility among developers, hospitals and clinicians in a manner that protects patients without chilling beneficial innovation.

I. Introduction

Medicine has always absorbed new instruments, from the stethoscope to the CT scanner, but AI differs in kind. A conventional instrument extends a clinician's senses; an AI system performs part of the clinician's reasoning. A deep-learning model that screens a chest radiograph, a risk score that ranks inpatients for sepsis and a language model that drafts a treatment plan each generate a recommendation that a human may accept, adjust or ignore. The scale is already substantial¹. The public list of AI-enabled devices maintained by the United States Food and Drug Administration (FDA) recorded 1,614 authorisations by the end of June 2026, of which 1,230, or 76 per cent, were radiology devices.² India's regulator has only recently begun to address software of this kind specifically.³

The same technologies have failed in instructive ways. An independent external validation of the widely deployed Epic Sepsis Model, covering 38,455 hospitalisations, found an area under the curve of 0.63, well below the 0.76–0.83 reported by its developer, and found that the model failed to identify 67 per cent of patients with sepsis while generating alerts for 18 per cent of all hospitalised patients.⁴ A widely used American algorithm for allocating care-management resources was shown to understate the needs of Black patients because it used healthcare costs as a proxy for health need.⁵ These episodes show that the legal problem is not hypothetical, and that harm from clinical AI is frequently systemic, arising from design, validation and

¹ US Food and Drug Administration, 'Artificial Intelligence-Enabled Medical Devices' <<https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices>> accessed 1 September 2026.

² 'Top 10 AI Vendors by FDA Approvals' (*The Imaging Wire*, 13 September 2026) <<https://theimagingwire.com/2026/09/13/radiology-maintained-its-lead-in-fda-approvals>> accessed 1 September 2026 (reporting the cumulative figures to the end of June 2026).

³ Central Drugs Standard Control Organisation, *Draft Guidance Document on Medical Device Software* (21 October 2025).

⁴ Andrew Wong and others, 'External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients' (2021) 181 JAMA Internal Medicine 1065.

⁵ Ziad Obermeyer and others, 'Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations' (2019) 366 Science 447.

deployment choices rather than from the lapse of a single clinician.

Law must answer three connected questions. The first is what a system must satisfy before it may be placed on the market. The second is how it must be monitored, explained and governed once in use. The third is who compensates the patient when harm occurs, and on what basis. Jurisdictions have answered these questions differently. India has not yet legislated. Its courts continue to apply the standard of professional negligence articulated in *Jacob Mathew v State of Punjab*,⁶ under which a practitioner is liable only where she fails to act with the ordinary skill of a competent member of her profession; its consumer law holds hospitals answerable for deficiency in service; and its regulators have begun to fit AI within medical-device and data-protection law. Policy documents, including the India AI Governance Guidelines issued by the Ministry of Electronics and Information Technology (MeitY) in November 2025, expressly prefer existing law and sectoral regulators to a standalone AI statute.⁷

This paper adopts a doctrinal and comparative method. It relies on primary sources, namely statutes, regulations, regulatory guidance and judgments, and, for empirical claims, on peer-reviewed studies and official data. The law is stated as at 6 October 2026. Part II identifies the technological features that strain existing doctrine. Parts III, IV and V examine India, the European Union (EU) and the United States (US) respectively. Part VI compares the three systems, Part VII proposes reforms for India and Part VIII concludes.

II. AI in Diagnosis and Treatment: Technological Features and Legal Problems

Clinical AI is not a single technology. It is useful to distinguish assistive systems, which present information or a recommendation that a clinician must independently evaluate, from autonomous systems, which produce a diagnosis without contemporaneous human review. The first autonomous diagnostic system authorised in the US, the IDx-DR system for detecting diabetic retinopathy in primary-care settings, was granted marketing authorisation in April 2018.⁸ Most deployed systems remain assistive, and the legal significance of the distinction lies in where professional judgment is located. A further distinction separates ‘locked’ algorithms from adaptive ones that continue to learn after deployment, which challenge any regulatory model premised on the approval of a fixed product.

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

⁷ Ministry of Electronics and Information Technology, *India AI Governance Guidelines* (November 2025).

⁸ US Food and Drug Administration, ‘FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems’ (Press Release, 11 April 2018).

Four features strain existing doctrine. The first is opacity: patients and courts cannot readily reconstruct why a model produced a given output, which complicates proof of breach and causation. The second is data-dependent bias, illustrated by the cost-proxy algorithm discussed above.⁹ The third is variability of performance across settings and over time. A model validated in one population may perform poorly in another, as the sepsis study shows, and this is of particular relevance to India, whose population, disease profile and imaging infrastructure differ from the datasets that dominate the literature; the ICMR's own guidelines stress the need for representative Indian data.¹⁰ The fourth is automation bias, the documented tendency of users to over-rely on automated advice; a systematic review found that it can lead clinicians to accept erroneous recommendations that they would otherwise have rejected.¹¹ The EU's AI Act now requires human overseers of high-risk systems to remain aware of this tendency.¹² These features produce a problem of many hands. The developer designs and trains the model, the hospital selects, integrates and maintains it, and the clinician relies on it at the bedside. Price, Gerke and Cohen have mapped the circumstances in which a physician's decision to follow or reject an AI recommendation may expose her to liability, observing that the answer depends on whether the recommendation reflects the standard of care, while the position of developers and institutions is comparatively uncertain.¹³ The World Health Organization's guidance on the ethics and governance of AI for health likewise insists that accountability mechanisms keep humans answerable for AI-assisted decisions.¹⁴ A sound legal framework must therefore allocate responsibility among three actors, namely developer, deploying institution and clinician, rather than concentrate it on the last of them.

III. The Indian Framework: Professional Negligence, Institutional Liability and an Incomplete Regulatory Overlay

Indian law imposes liability on a medical practitioner who breaches a duty of care. In *Jacob Mathew* the Supreme Court adopted a modified *Bolam* standard, holding that a practitioner is negligent only where she fails to exercise the ordinary skill of a competent professional in her

⁹ Obermeyer and others (n 4).

¹⁰ Indian Council of Medical Research, *Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare* (ICMR 2023).

¹¹ Kate Goddard, Abdul Roudsari and Jeremy C Wyatt, 'Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators' (2012) 19 *Journal of the American Medical Informatics Association* 121.

¹² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689 (AI Act), art 14(4)(b).

¹³ W Nicholson Price II, Sara Gerke and I Glenn Cohen, 'Potential Liability for Physicians Using Artificial Intelligence' (2019) 322 *JAMA* 1765.

¹⁴ World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance* (WHO 2021).

field, and that criminal liability requires gross negligence or recklessness.¹⁵ The Court has since reaffirmed the reasonable-practitioner standard and its application as at the time of treatment.¹⁶ These principles now sit within the Bharatiya Nyaya Sanhita 2023, section 106(1) of which prescribes a reduced maximum term of two years for a registered medical practitioner who causes death by a negligent act in the course of a medical procedure.¹⁷ Courts ordinarily look to expert evidence to establish breach, although this is not an invariable requirement where negligence is manifest.¹⁸

Applied to AI, these doctrines yield a coherent but incomplete answer. A clinician who relies on an approved decision-support system whose limits she understands, and who exercises independent judgment, is unlikely to be negligent merely because the system erred; *Jacob Mathew* protects a practitioner who follows an accepted practice, and the use of a validated tool is increasingly such a practice. Conversely, a clinician who abdicates judgment to an output plainly inconsistent with the clinical picture, or who uses an unvalidated tool, falls below the standard. The Telemedicine Practice Guidelines 2020 reinforce this allocation. They prohibit AI-based platforms from counselling patients or prescribing medicines, and provide that while AI-based decision-support systems may assist a registered medical practitioner in evaluation, diagnosis or management, the final prescription or counselling must be delivered by the practitioner.¹⁹ Professional responsibility therefore remains with the human clinician. The difficulty is that the *Bolam* inquiry presupposes a body of professional opinion about what competent practitioners do. For tools whose reliability a clinician cannot independently assess, that body of opinion is only beginning to form, and an expert witness may be unable to say what an ordinary clinician should have done with an opaque output.

Hospital liability fills part of the gap. In *Achutrao Haribhau Khodwa v State of Maharashtra* the Supreme Court refused to let the State escape liability for negligence in a government hospital,²⁰ *Indian Medical Association v VP Shantha* brought medical services rendered for consideration within consumer law,²¹ and *Spring Meadows Hospital v Harjol Ahluwalia* confirmed a hospital's liability in proceedings arising from negligent treatment of a child.²²

¹⁵ *Jacob Mathew* (n 5) [48]; *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582 (QB).

¹⁶ *Arun Kumar Manglik v Chirayu Health and Medicare Pvt Ltd* (2019) 7 SCC 401.

¹⁷ Bharatiya Nyaya Sanhita 2023, s 106(1).

¹⁸ *Dr Harish Kumar Khurana v Joginder Singh* (2021) 10 SCC 291; *V Kishan Rao v Nikhil Super Speciality Hospital* (2010) 5 SCC 513.

¹⁹ Ministry of Health and Family Welfare and NITI Aayog, *Telemedicine Practice Guidelines: Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine* (25 March 2020).

²⁰ *Achutrao Haribhau Khodwa v State of Maharashtra* (1996) 2 SCC 634.

²¹ *Indian Medical Association v VP Shantha* (1995) 6 SCC 651.

²² *Spring Meadows Hospital v Harjol Ahluwalia* (1998) 4 SCC 39.

Savita Garg v Director, National Heart Institute recognised the evidentiary difficulty of a patient who lacks access to the hospital's internal records.²³ The Consumer Protection Act 2019 defines 'deficiency' and 'service' broadly, and so supplies a forum in which a patient can proceed against a hospital without identifying a single negligent doctor.²⁴ This institutional lens is directly relevant to clinical AI, because the decisions that determine whether a system is safe, namely whether to procure it, whether to validate it on local data, how to integrate it into workflow and how to monitor its performance, are made by the institution rather than by the bedside clinician. A hospital that deploys an unvalidated sepsis-prediction tool, or that fails to train its staff in its limits, may be directly answerable for deficiency in service independently of any individual practitioner.

The product side is regulated through the Drugs and Cosmetics Act 1940 and the Medical Devices Rules 2017. Since 1 April 2020, a notification of 11 February 2020 has brought medical devices generally, expressly including software intended for medical purposes, within the definition of 'drug'.²⁵ Devices are classified in Classes A to D by risk and licensed by the Central Drugs Standard Control Organisation (CDSCO). Because the Rules were drafted with hardware in mind, they say little about adaptive algorithms. On 21 October 2025 the CDSCO therefore released a draft guidance on medical device software, distinguishing software in a medical device from software as a medical device and proposing risk-based classification, quality-management requirements and an algorithm change protocol for AI that updates after deployment.²⁶ Press reports in July 2026 indicate that the framework has since been formalised, with Class C and D software requiring full technical dossiers and clinical data;²⁷ the primary notification should be consulted for the final text.

Soft law supplements this regime. The ICMR's 2023 guidelines set out ten patient-centric principles, including human oversight, accountability, informed consent and representative datasets, but they are not binding.²⁸ NITI Aayog's National Strategy for Artificial Intelligence of 2018 identified healthcare as a priority sector,²⁹ and MeitY's 2025 guidelines reject a standalone AI statute in favour of existing law, sectoral regulators and seven guiding principles, while contemplating targeted amendments to clarify the liability of AI developers, deployers

²³ *Savita Garg v Director, National Heart Institute* (2004) 8 SCC 56.

²⁴ Consumer Protection Act 2019, ss 2(11), 2(42).

²⁵ Ministry of Health and Family Welfare, Notification S.O. 648(E) (11 February 2020); Medical Devices Rules 2017, G.S.R. 78(E) (31 January 2017).

²⁶ CDSCO (n 2).

²⁷ 'CDSCO's New Rules: AI Diagnostic Software Now Needs Medical Device Licence' (*The420.in*, 22 July 2026) <<https://the420.in/cdsco-ai-medical-software-device-classification-india>> accessed 1 September 2026.

²⁸ ICMR (n 9).

²⁹ NITI Aayog, *National Strategy for Artificial Intelligence* (June 2018).

and users.³⁰

Autonomy and privacy supply a further layer. *Justice KS Puttaswamy (Retd) v Union of India* recognised privacy as a fundamental right,³¹ and *Samira Kohli v Dr Prabha Manchanda* requires consent that is informed as to the nature of a procedure and its material risks.³² Whether the use of an AI system in a patient's diagnosis is itself a material fact requiring disclosure is unsettled, although the ICMR guidance suggests that it should be. The Digital Personal Data Protection Act 2023 requires a data fiduciary to ensure the completeness, accuracy and consistency of personal data likely to be used to make a decision affecting the data principal,³³ but, unlike article 22 of the EU's General Data Protection Regulation, it confers no right to contest or obtain human review of an automated decision. The Digital Personal Data Protection Rules 2025, notified in November 2025, bring the Act into force in phases, with most substantive obligations taking effect in May 2027.³⁴

Four gaps follow. First, the product-liability chapter of the Consumer Protection Act applies to a 'product' defined by reference to goods capable of delivery,³⁵ and it is doubtful that stand-alone software or a cloud-hosted model falls within it, leaving the developer's liability to general tort and contract. Second, nothing requires a developer or hospital to preserve logs sufficient for a court to reconstruct an AI-assisted decision. Third, there is no duty to disclose to patients that AI contributed to their diagnosis. Fourth, the regulatory perimeter is unclear for generative and general-purpose systems used informally by clinicians, which the Medical Devices Rules were never designed to capture.

IV. The European Union: A Horizontal, Risk-Based Regime Layered on Device Law

The EU has chosen comprehensive horizontal regulation. Regulation (EU) 2024/1689, the AI Act, entered into force on 1 August 2024 and classifies AI systems by risk.³⁶ Its application to clinical AI runs principally through article 6(1) and Annex I. An AI system is high-risk where it is, or is a safety component of, a product covered by listed Union harmonisation legislation and that product must undergo third-party conformity assessment. The Medical Device

³⁰ MeitY (n 6).

³¹ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

³² *Samira Kohli v Dr Prabha Manchanda* (2008) 2 SCC 1.

³³ Digital Personal Data Protection Act 2023, s 8(3).

³⁴ Digital Personal Data Protection Rules 2025 (notified November 2025).

³⁵ Consumer Protection Act 2019, s 2(33) and ch VI (ss 82–87).

³⁶ AI Act (n 11) art 113.

Regulation (MDR) and the In Vitro Diagnostic Regulation (IVDR) are listed in Annex I.³⁷ Because rule 11 of Annex VIII to the MDR classifies software providing information used for diagnostic or therapeutic decisions as at least Class IIa, rising to Class IIb where error may cause serious deterioration or surgical intervention and to Class III where it may cause death or irreversible deterioration, most diagnostic AI requires notified-body involvement and is therefore high-risk.³⁸ In *SNITEM and Philips France* the Court of Justice held that decision-support software may itself be a medical device where it is intended for use in relation to the medical care of an individual patient.³⁹ Annex III separately lists emergency healthcare patient-triage systems as high-risk.⁴⁰

High-risk providers must establish a risk-management system, apply data-governance practices to training and validation data, maintain technical documentation and automatic logging, provide transparency to deployers, enable effective human oversight and achieve appropriate accuracy, robustness and cybersecurity.⁴¹ Deployers, a category that includes hospitals, must use systems in accordance with their instructions, assign oversight to competent and trained persons and retain the logs under their control.⁴² Persons affected by decisions based on certain Annex III systems have a right to a clear and meaningful explanation,⁴³ and infringements of operator obligations attract administrative fines of up to EUR 15 million or three per cent of worldwide annual turnover.⁴⁴

The timetable has shifted. The AI Act originally applied its high-risk rules from 2 August 2026 for Annex III systems and 2 August 2027 for products covered by Annex I. Regulation (EU) 2026/1744, the Digital Omnibus on AI, approved by the Council on 29 June 2026 and published in the Official Journal in July 2026, defers the Annex III obligations to 2 December 2027 and the obligations for AI embedded in Annex I products, including medical devices, to 2 August 2028.⁴⁵ The substantive architecture is unchanged. Until then, medical AI in the EU will be

³⁷ AI Act (n 11) art 6(1) and annex I, section A; Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices [2017] OJ L117/1 (MDR); Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices [2017] OJ L117/176 (IVDR).

³⁸ MDR (n 36), annex VIII, rule 11; Medical Device Coordination Group, *MDCG 2019-11: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 and Regulation (EU) 2017/746* (October 2019, rev June 2025).

³⁹ Case C-329/16 *Syndicat national de l'industrie des technologies médicales (SNITEM) and Philips France v Ministre des Affaires sociales et de la Santé* ECLI:EU:C:2017:947.

⁴⁰ AI Act (n 11) annex III, point 5(d).

⁴¹ AI Act (n 11) arts 9–15.

⁴² AI Act (n 11) art 26.

⁴³ AI Act (n 11) art 86.

⁴⁴ AI Act (n 11) art 99(4).

⁴⁵ Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) [2026] OJ L2026/1744; Council of the European Union, 'Artificial intelligence: Council gives final green light to simplify and streamline rules' (Press Release, 29 June 2026).

regulated principally through the MDR and IVDR, with their requirements for clinical evaluation and post-market surveillance.

The General Data Protection Regulation (GDPR) overlays the AI Act. Health data are special-category data whose processing is prohibited unless an exception applies, including medical diagnosis and the provision of health care under a professional's responsibility.⁴⁶ Article 22 restricts decisions based solely on automated processing that produce legal or similarly significant effects. In *SCHUFA Holding (Scoring)* the Court of Justice held that the automated establishment of a probability value is itself an automated decision where a third party draws strongly on it in deciding,⁴⁷ reasoning that arguably extends to a clinical risk score on which a hospital relies heavily. In *Dun & Bradstreet Austria* the Court held that a data subject is entitled to an explanation of the procedure and principles actually applied in reaching an automated decision, subject to a balancing against trade secrets.⁴⁸ Data protection impact assessments are required for high-risk processing,⁴⁹ and the European Health Data Space Regulation additionally structures the secondary use of health data for purposes such as AI development.⁵⁰ Liability remains the least harmonised element. The Commission's proposed AI Liability Directive, which would have eased the proof of fault, was withdrawn, with formal notice published in October 2025,⁵¹ so fault-based medical liability remains a matter for national law. Strict liability, however, is being modernised. Directive (EU) 2024/2853 replaces the 1985 Product Liability Directive, expressly treats software, including AI systems, as a 'product', extends compensable damage to medically recognised psychological harm, empowers courts to order disclosure of evidence and establishes rebuttable presumptions of defect and causation where technical complexity makes proof excessively difficult.⁵² The reform places developers of clinical AI under strict liability, and its disclosure and presumption rules speak directly to the problem of opacity. It leaves hospital and clinician negligence to national law, and leaves

2026); 'EU AI Act unpacked #34: The final Digital Omnibus on AI' (*Freshfields Technology Quotient*, 2026) <<https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-ai-act-unpacked-34-the-final-digital-omnibus-on-ai-key-amendments-to-the-a-102nber>> accessed 3 September 2026.

⁴⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, arts 9(1), 9(2)(h).

⁴⁷ Case C-634/21 *SCHUFA Holding (Scoring)* ECLI:EU:C:2023:957.

⁴⁸ Case C-203/22 *Dun & Bradstreet Austria* ECLI:EU:C:2025:117.

⁴⁹ GDPR (n 45) art 35.

⁵⁰ Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space [2025] OJ L2025/327.

⁵¹ Commission, 'Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM(2022) 496 final; 'Withdrawal of Commission proposals' [2025] OJ C/2025/5423 (6 October 2025).

⁵² Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L2024/2853, arts 4(1), 6, 9–10. Member States must transpose the Directive by 9 December 2026.

open how continuously learning systems are to be assessed for defect.

V. The United States: Device Regulation, Tort Liability and State Experimentation

The US has no general AI statute. Clinical AI is regulated principally as a medical device under the Federal Food, Drug, and Cosmetic Act (FDCA), which defines a device broadly enough to include software intended for the diagnosis, mitigation, treatment or prevention of disease.⁵³ Devices reach the market through premarket approval, through De Novo classification for novel devices of low to moderate risk, or through 510(k) clearance on a showing of substantial equivalence to a predicate device.⁵⁴ The overwhelming majority of AI devices use the least demanding route: an analysis of the FDA's list of 1,614 authorisations found that about 96 per cent were cleared under section 510(k).⁵⁵ Clearance rests on equivalence to a predicate rather than on independently demonstrated clinical performance. To address adaptive software, the FDA issued final guidance in December 2024 on predetermined change control plans, which allow a manufacturer to obtain advance authorisation for specified algorithm modifications.⁵⁶ Congress narrowed the perimeter in the 21st Century Cures Act, which added section 520(o)(1)(E) to the FDCA. It excludes from the device definition certain clinical decision support software intended for health care professionals, provided that the software does not acquire, process or analyse medical images or signals and enables the professional to review independently the basis of its recommendations, so that she does not rely primarily on them.⁵⁷ The FDA's revised final guidance of January 2026 loosened its earlier reading, including by no longer treating a single recommendation as automatically disqualifying, while maintaining that software directed at patients or caregivers is generally a device and that time-critical functions are unlikely to qualify.⁵⁸ Commentators note that the guidance announces no new policy for consumer-facing tools such as health chatbots or symptom checkers.⁵⁹

Federal device law shapes tort claims through preemption. In *Riegel v Medtronic Inc* the

⁵³ Federal Food, Drug, and Cosmetic Act, 21 USC s 321(h).

⁵⁴ 21 USC ss 360e (premarket approval), 360c(f)(2) (De Novo), 360(k) (510(k) notification).

⁵⁵ 'What 1,614 FDA Authorizations Reveal About AI-Enabled Medical Devices' (*Sequenex*, 2026) <<https://sequenex.com/fda-ai-medical-device-authorizations-analysis>> accessed 3 September 2026.

⁵⁶ US Food and Drug Administration, *Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions: Final Guidance* (December 2024).

⁵⁷ 21st Century Cures Act, Pub L No 114-255, 130 Stat 1033 (2016) s 3060(a), adding FDCA s 520(o)(1)(E) (21 USC s 360j(o)(1)(E)).

⁵⁸ US Food and Drug Administration, *Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff* (January 2026), superseding the guidance of September 2022.

⁵⁹ Covington & Burling LLP, '5 Key Takeaways from FDA's Revised Clinical Decision Support (CDS) Software Guidance' (January 2026) <<https://www.cov.com/news-and-insights/insights/2026/01/5-key-takeaways-from-fdas-revised-clinical-decision-support-cds-software-guidance>> accessed 7 September 2026.

Supreme Court held that state-law claims challenging the safety or effectiveness of a device approved through premarket approval are preempted,⁶⁰ whereas in *Medtronic Inc v Lohr* it held that 510(k) clearance, which turns on equivalence rather than a safety review, did not preempt such claims.⁶¹ Because most clinical AI is cleared under section 510(k), preemption is less likely to bar claims against developers than it is for high-risk devices approved through premarket approval, although the position of De Novo devices is less settled.

Medical malpractice is a matter of state law. The standard of care is generally that of a reasonably prudent practitioner in like circumstances, and professional custom is evidence but not conclusive, since a whole industry may lag behind available precautions.⁶² The principle has obvious application to the question whether a failure to use, or to heed, validated AI may itself be negligent. *Canterbury v Spence* grounds informed consent in the patient's right to material information,⁶³ which would support disclosure of a material role for AI. As to institutions, *Darling v Charleston Community Memorial Hospital* established a hospital's direct duty to its patients, including a duty to supervise the quality of care,⁶⁴ and *Taylor v Intuitive Surgical Inc* held that the maker of the da Vinci surgical robot owed a duty under Washington's product-liability statute to warn the purchasing hospital, the gatekeeper between physician and device through its credentialing decisions, independently of any warning given to the surgeon.⁶⁵ Together these decisions describe a three-cornered allocation among clinician, hospital and manufacturer that maps closely onto clinical AI. The learned-intermediary doctrine, which ordinarily allows a manufacturer to discharge its duty to warn by informing the prescribing clinician, may still shield developers of assistive tools from direct patient claims, a result that *Taylor* qualifies but does not displace.

Litigation and enforcement are beginning to test AI-specific theories. In *Estate of Lokken v UnitedHealth Group Inc*, plaintiffs allege that an insurer used its nH Predict algorithm to curtail post-acute care coverage contrary to treating physicians' determinations. In February 2025 the District of Minnesota dismissed most claims on preemption grounds but allowed claims for breach of contract and of the implied covenant of good faith to proceed, and the court has since permitted discovery into how the algorithm works and whether it was designed to supplant physician decision-making.⁶⁶ In September 2024 the Texas Attorney General secured a

⁶⁰ *Riegel v Medtronic Inc* 552 US 312 (2008).

⁶¹ *Medtronic Inc v Lohr* 518 US 470 (1996).

⁶² *The TJ Hooper* 60 F 2d 737 (2d Cir 1932).

⁶³ *Canterbury v Spence* 464 F 2d 772 (DC Cir 1972).

⁶⁴ *Darling v Charleston Community Memorial Hospital* 211 NE 2d 253 (Ill 1965).

⁶⁵ *Taylor v Intuitive Surgical Inc* 389 P 3d 517 (Wash 2017).

⁶⁶ *Estate of Lokken v UnitedHealth Group Inc* No 0:23-cv-03514 (D Minn 13 February 2025); 'Court Allows Discovery Into Insurer's Use of AI to Deny Claims' (*Hunton Insurance Recovery Blog*, 2025) <<https://www.hunton.com/hunton->

settlement from Pieces Technologies, whose generative-AI clinical summaries were marketed with a claimed ‘severe hallucination rate’ below one in 100,000, a metric the Attorney General found likely inaccurate.⁶⁷

States are legislating where federal law is silent. California requires health facilities to disclose when patient communications on clinical matters are generated by generative AI without clinician review (AB 3030) and restricts the use of AI alone to deny, delay or modify care on grounds of medical necessity (SB 1120);⁶⁸ Illinois has restricted the provision of therapy by AI;⁶⁹ and Colorado is reported to have replaced its 2024 AI Act with a narrower automated-decision statute in May 2026.⁷⁰ Federal anti-discrimination law reaches clinical AI through the 2024 rule under section 1557 of the Affordable Care Act, which requires covered entities to make reasonable efforts to identify and mitigate discrimination risks in patient-care decision-support tools,⁷¹ and the Health Insurance Portability and Accountability Act governs the privacy of the data used to train and operate such tools.⁷² This activity coincides with a federal effort to displace state AI laws: an executive order of 11 December 2025 directs the pursuit of a uniform national policy framework, and its effect on health-specific state legislation remains uncertain.⁷³

VI. Comparative Analysis: Three Models of Governing Clinical AI

All three systems treat diagnostic AI as a regulated medical product, but their architectures differ. The EU layers AI-specific obligations on device conformity assessment, the US applies device law with a statutory carve-out for professional-facing decision support, and India applies device law by notification while it elaborates software-specific guidance. The Indian and American models share a reliance on the device concept, which leaves outside the perimeter systems that are not devices: clinician-facing tools within the US carve-out, and general-purpose models used informally by Indian clinicians. The EU’s horizontal approach captures such systems in principle, at the price of complexity and, as the Digital Omnibus shows, of

[insurance-recovery-blog/court-allows-discovery-into-insurers-use-of-ai-to-deny-claims](#)> accessed 8 September 2026.

⁶⁷ Office of the Attorney General of Texas, ‘Attorney General Ken Paxton Reaches Settlement in First-of-its-Kind Healthcare Generative AI Investigation’ (Press Release, September 2024) <<https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-settlement-first-its-kind-healthcare-generative-ai-investigation>> accessed 8 September 2026.

⁶⁸ Cal Health & Saf Code ss 1339.75 (AB 3030), 1367.01 (SB 1120).

⁶⁹ Wellness and Oversight for Psychological Resources Act (Illinois HB 1806, 2025), effective 1 August 2025.

⁷⁰ ‘U.S. AI Law – 2026 Midyear State Update’ (*Privacy World*, September 2026) <<https://www.privacyworld.blog/2026/09/u-s-ai-law-2026-midyear-state-update>> accessed 15 September 2026.

⁷¹ 45 CFR s 92.210.

⁷² Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191; 45 CFR pts 160, 164.

⁷³ Executive Order, ‘Ensuring a National Policy Framework for Artificial Intelligence’ (11 December 2025).

implementation delay. Adaptivity is addressed most concretely in the US through predetermined change control plans, is proposed in India through the algorithm change protocol, and is handled in the EU through post-market monitoring and the AI Act's treatment of pre-determined changes in conformity assessment.

The contrast can be summarised across six dimensions. As to core instruments, India relies on the Medical Devices Rules 2017 (which have covered software since 2020), the CDSCO's draft software guidance of 2025, the ICMR guidelines of 2023 and the Digital Personal Data Protection Act 2023; the EU on the AI Act, the MDR and IVDR, the GDPR and Directive 2024/2853; and the US on the FDCA, section 520(o)(1)(E) added by the Cures Act, FDA guidance and state tort and statute law. As to premarket control, India licenses software through the CDSCO in Classes A to D; the EU requires notified-body conformity assessment, with the AI Act's high-risk rules applying to Annex I products from 2 August 2028; and the US permits entry through 510(k) clearance, De Novo classification or premarket approval, while excluding non-device decision support altogether. As to adaptive AI, India's approach is a draft algorithm change protocol, the EU's is post-market monitoring and the treatment of pre-determined changes, and the US's is the predetermined change control plan of 2024.

As to developer liability, India offers only general tort and contract, with the application of the Consumer Protection Act 2019 to software unclear; the EU will impose strict liability for software from December 2026; and the US applies state product-liability law subject to preemption for devices approved through premarket approval. As to the duties of hospitals, India relies on deficiency in service under the Consumer Protection Act 2019 and on *Spring Meadows* and *Savita Garg*; the EU on the deployer duties in article 26 of the AI Act and national negligence law; and the US on corporate negligence under *Darling* and the duty to warn the hospital recognised in *Taylor*. As to explanation and consent, India has non-binding ICMR guidance and section 8(3) of the Digital Personal Data Protection Act; the EU has articles 15 and 22 of the GDPR and article 86 of the AI Act; and the US has informed-consent doctrine under *Canterbury* and state disclosure laws.

On liability the EU has moved furthest on developers, the US relies on state tort law with unsettled preemption, and India applies professional negligence and consumer law without any rule directed at developers. Clinicians remain professionally responsible in all three. Each system also recognises, to different degrees, an independent responsibility of the institution: *Darling* and *Taylor* in the US,⁷⁴ the hospital-liability decisions of the Indian Supreme Court,⁷⁵

⁷⁴ *Darling* (n 63); *Taylor* (n 64).

⁷⁵ *Spring Meadows* (n 21); *Savita Garg* (n 22).

and the deployer obligations of article 26 of the AI Act. India's distinctive position is that it has an accessible consumer forum for institutional claims but a weak basis for reaching developers. On explanation and disclosure, the EU has articles 15 and 22 of the GDPR, article 86 of the AI Act and the case law of the Court of Justice; the US has informed-consent doctrine and a growing set of state disclosure statutes; India has only non-binding ICMR guidance and the accuracy duty in section 8(3) of the Digital Personal Data Protection Act.

Four lessons emerge. First, risk-based tiering is indispensable, because the same legal burden cannot sensibly be placed on a scheduling tool and on an autonomous diagnostic system. Second, obligations must attach to the deploying institution as well as the developer and the clinician, since validation, integration and monitoring occur at institutional level. Third, liability reform must confront evidence: opacity makes disclosure duties, logging and rebuttable presumptions as important as the substantive standard of liability. Fourth, the experience of the EU, whose deadlines have slipped, and of the US, where federal and state initiatives collide, cautions against both over-ambitious horizontal legislation and prolonged reliance on non-binding guidance. India's context, with a large public-hospital sector, extensive telemedicine and uneven institutional capacity, counsels proportionality.

VII. Towards an Indian Framework: Proposals for Reform

First, the CDSCO's software framework should be finalised and placed on a secure statutory footing through rules under the Drugs and Cosmetics Act 1940 or successor legislation. It should require risk-tiered clinical evidence, local validation on representative Indian data for higher-risk systems, an algorithm change protocol for adaptive models, post-market surveillance and mandatory incident reporting.

Second, the National Medical Commission, established under the National Medical Commission Act 2019, should issue professional-conduct guidance on the use of AI that builds on the Telemedicine Practice Guidelines. It should state that reliance on a validated tool is not in itself negligent, that unquestioning reliance on an output inconsistent with the clinical picture is, and that clinicians must document material reliance on, and departure from, AI recommendations. This preserves the clinician's non-delegable duty while giving the *Bolam* inquiry a defined professional practice against which to operate.

Third, Indian law should recognise an independent institutional duty on hospitals that deploy clinical AI, consistent with *Spring Meadows* and *Savita Garg*. That duty should cover procurement due diligence, validation on the institution's own patient population, staff training, performance monitoring, incident reporting and the assignment of competent human oversight.

It can be given content through registration standards under the Clinical Establishments (Registration and Regulation) Act 2010 and applied by consumer fora as part of the assessment of deficiency in service.

Fourth, the definition of ‘product’ in the Consumer Protection Act 2019 should be amended to include software and AI systems, so that the product-liability chapter reaches developers. Disclosure-of-evidence and rebuttable-presumption rules modelled on articles 9 and 10 of the EU’s Product Liability Directive, adapted to the procedure of consumer commissions, would address the informational asymmetry that *Savita Garg* identified.⁷⁶

Fifth, transparency obligations should be made binding. Developers and hospitals should retain logs sufficient to reconstruct an AI-assisted decision; patients should be told when AI materially contributes to diagnosis or treatment, so that consent under *Samira Kohli* is informed;⁷⁷ and the data-protection framework should be extended, through rules or amendment, to give patients a right to human review of significant automated health decisions, as article 22 of the GDPR does.

Sixth, equity must be built into regulation. Developers should be required to report performance by relevant subgroups, such as age, sex, region and imaging equipment, and high-risk systems should be periodically audited for bias, giving effect to the ICMR’s call for representative data. Finally, proportionality should govern the whole: low-risk administrative tools should be exempt from heavy obligations, and a regulatory sandbox could allow supervised testing of novel systems, so that compliance burdens do not entrench large incumbents or deter Indian developers.

VIII. Conclusion

AI-based diagnosis and treatment expose the limits of a legal order organised around the individual clinician and the static device. The EU has built the most elaborate regulatory architecture but has had to defer its application. The US relies on device regulation, a contested carve-out for decision support, state tort law and fragmented state legislation. India has the beginnings of a regime but not yet its legal foundations: negligence law that protects the clinician, consumer law that reaches the hospital, and device and data-protection rules that are still evolving.

India need not and should not copy either model. Its task is to preserve the clinician’s professional responsibility, to recognise that hospitals are the institutions that choose, validate

⁷⁶ Directive (EU) 2024/2853 (n 51) arts 9–10; *Savita Garg* (n 22).

⁷⁷ *Samira Kohli* (n 31).

and monitor clinical AI, to bring developers within a liability regime suited to software, and to make explanation, logging, consent and fairness enforceable rather than aspirational. Because clinical AI is delivered through institutions, responsibility for its safety must be institutional as well as individual. Reforms along these lines would allow Indian patients to benefit from AI-assisted care without bearing alone the risks of technologies they cannot see inside.

