INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 3 | 2026 Art. 32

Algorithmic Error and Medical Negligence in India: Navigating the Regulatory Vacuum in AI-Driven Healthcare

N. Shanmukhi Pravalika
LLM Student,
Amity Law School, Amity University, Bengaluru

Sahaya Jenifer B J
LLM Student,
Amity Law School, Amity University, Bengaluru

Recommended Citation
N. Shanmukhi Pravalika and Sahaya Jenifer B J, *Algorithmic Error and Medical Negligence in India: Navigating the Regulatory Vacuum in AI-Driven Healthcare,* 5 IJHRLR 457-471 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Algorithmic Error and Medical Negligence in India: Navigating the Regulatory Vacuum in AI-Driven Healthcare

ABSTRACT

The malfunctioning of AI-enabled healthcare systems exposes a pronounced structural gap within India's medico-legal framework, wherein established doctrines of medical negligence struggle to accommodate automated decision-making. Indian law, historically grounded in human-centric notions of duty of care, standard of care, and proximate causation, does not clearly attribute liability when diagnostic or therapeutic errors arise from machine-learning systems—particularly in complex, multi-stakeholder environments involving clinicians, hospitals, software developers, and data providers. Existing legal frameworks, including the Consumer Protection Act, 2019, and negligence principles shaped by the Indian Medical Council and judicial precedents, remain largely ill-suited to opaque and adaptive AI systems, whose functioning often resists conventional tests of foreseeability. This regulatory inadequacy is compounded by the absence of a dedicated AI liability regime and the fragmented interplay between statutes such as the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and sector-specific medical device and pharmaceutical regulations. The resulting legal uncertainty is particularly evident in questions of causation and evidentiary burden. Claimants face significant challenges in reconstructing algorithmic decision-making processes and in demonstrating deviation from an evolving, technology-informed standard of care. Comparative regulatory approaches—such as the U.S. Food and Drug Administration's Software as a Medical Device (SaMD) framework and emerging European liability models—underscore the need for India to adopt mechanisms ensuring algorithmic transparency, mandatory error-reporting, and a calibrated liability structure that balances innovation with patient safety. Absent such reform, India risks entrenching a regulatory vacuum in which algorithmic errors are insufficiently deterred, accountability remains diffuse, and patients are left navigating an uncertain space between traditional medical malpractice and unregulated AI-driven harm.

KEYWORDS

Algorithmic, Negligence, Liability, Healthcare, Regulation

1. INTRODUCTION

The breakdown of the AI-enabling healthcare systems reveals a glaring structural flaw in India's medico legal system. Existing medical negligence doctrines, which are based primarily on people-centred ideas of duty, standard of care and immediate action, are incapable of facilitating automated and artificial decision-making, especially when diagnostic or therapeutic errors emerge from systems based on machine learning rather than from individuals. If they happen to be in complicated, multifaceted situations involving doctors, hospitals, software engineers and data vendors, Indian law does not clearly lay the blame for algorithmic failures, leaving victims at the crossroads of tort, consumer law and nascent data security norms. However, existing Indian legislation, such as the Consumer Protection Act, 2019,[1] is still more in need of adaptation to opaque and adaptive AI systems as the negligence principles introduced along court decisions like *Jacob Mathew v. State of Punjab* and the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations.

The opacity of "black box" neural networks and the challenges of reconstructing algorithmic decision pathways undermine conventional tests of foreseeability and breach of standard of care — tests that, based on observable, explainable human conduct, work best in systems. This inadequacy of regulation becomes exacerbated when you consider the lack of a regulatory environment of its own and the fragmented and overlapping regulation of the Information Technology Act, 2000,[2] the Digital Personal Data Protection Act, 2023[3] and related data regulations specific to the specific areas of health-related devices and pharmaceutical products.

The resulting legal uncertainty is most apparent in issues of causation and evidentiary burden. In AI mediated medical error cases, claimants have significant evidentiary obstacles to rebuild the algorithmic decision-making process, gain access to training data and logs of the model and show that a departure from a changing technology-driven standard of care occurred. And healthcare professionals might continue to cloak their actions in the "algorithm did it" cloak, reducing professional accountability. These comparative experiments—both those of the U.S. Food and Drug Administration's Software as a Medical Device (SaMD) framework and the European Union's risk-based AI Act and medical device regulations—underscore the imperative for India to enact mechanisms governing algorithmic transparency, mandatory error

[1] Consumer Protection Act, No. 35 of 2019, Gazette of India, Extra., pt. II-sec. 1 (Aug. 9, 2019).
[2] Information Technology Act, No. 21 of 2000, Gazette of India, Extra., pt. II-sec. 1 (June 9, 2000).
[3] Digital Personal Data Protection Act, No. 18 of 2023, Gazette of India, Extra., pt. II-sec. 1 (Aug. 11, 2023)

reporting, and a calibrated liability framework that effectively promotes the balance between innovation and patient safety.

Absent such reform, India risks entrenching a regulatory vacuum in which algorithmic errors are insufficiently deterred, accountability remains diffuse, and patients are left navigating an uncertain space between traditional medical malpractice and unregulated AI driven harm.

This paper therefore seeks to:

- Identify the doctrinal and statutory vacuums in the Indian medico legal landscape of algorithmic error;
- Explore existing doctrines of liability (negligence, product liability, consumer law) which clash and intersect with AI driven decision making;
- Assess the disjointed interface between Consumer Protection Act, 2019, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and medical device-specific laws; and
- Recommend a normative approach drawn from some of the comparative models which allocates liability between stakeholders, increases evidentiary rights and implicates accountability mechanisms in AI-supported systems of healthcare.

2. CONCEPTUALIZING ALGORITHMIC ERROR IN HEALTHCARE

Healthcare AI systems algorithmic errors significantly differ from human errors; they need a set of concepts and frameworks to analyse what went wrong and how to fix it. This answer introduces core definitions along with error classes, and also provides a socio-technical viewpoint of AI-mediated care.

2.1 Algorithmic vs. Human Error

Algorithmic error encompasses any inaccurate output from an AI system that deviates from expected performance or outputs, resulting in potentially dangerous patient effects if undetected. Human error is an unintentional deviation from safe practice resulting from slips (e.g., distractions), lapses (e.g., faulty memory), or mistakes (e.g., knowledge gaps). Human errors often result from individual causes like fatigue or fixation, while algorithmic errors result from systemic issues with data, models, or deployment environments.

2.2 Types of AI-Health Errors

Medical AI systems can do so well, but the underlying mistakes they produce (false positives) and false negatives (missing disease) can have a long-lasting impact on diagnostics. Bias happens when models include spurious correlations like protected characteristics which leads to differences between subpopulations. [4]Concept drift occurs when real-world data deviates from training distributions, compromising performance over time. This process is called under-calibration (also known as calibration drift) in which predicted probabilities are misaligned with observed outcomes, thus overestimating (or underestimating) risks in new population segments.

Error Type	Description	Healthcare Impact Example
False Positives/Negatives	Misclassification of cases	Unnecessary biopsies or missed sepsis
Bias	Systematic disparities	Lower accuracy for underrepresented groups
Drift	Performance decay post-deployment	Reduced prognostic reliability in varying hospitals
Under-calibration	Mismatched probability estimates	Inequitable triage decisions

2.3 Socio-Technical Conception

AI-mediated healthcare operates as a socio-technical system, where technology interacts with people, workflows, environments, and organizations. Errors emerge not just from algorithms but from poor integration, e.g., clinician mistrust of "black-box" outputs or workflow mismatches. Key considerations include AI's fit within clinical temporality, transparency for trust-building, and holistic risk assessment across system elements like tasks and tools. This framework urges audits for hidden failure modes, such as subgroup harms, beyond isolated

[4] Micah Arbeit, Real-World Evaluation & Drift Monitoring for Health AI (Jan. 21, 2026)

technical fixes.

3. MEDICAL NEGLIGENCE UNDER INDIAN LAW

Indian law under medical negligence forms the core of holding healthcare providers responsible and tort principles and leading judicial precedents continue to evolve in the context of healthcare providers. This chapter examines the essential factors such as duty of care, standards, causation, major case law and challenges created when bringing AI into practice.

3.1 Duty of Care and Standard

The doctor-patient relationship also establishes a duty of care among doctors: doctors must provide reasonable skill, knowledge, and diligence and exercise the skill demanded of such a competent professional. Breach occurs if this duty is not met and found satisfying through the three-stage test: existence of duty, breach of duty, and injury resulted from it. Proximate causation requires a direct cause: a breach of it must be followed by injury—not just a possibility, as clarified in *Achutrao Haribhau Khodwa v. State of Maharashtra*.[5]

3.2 Judicial Tests and Precedents

Jacob Mathew v. State of Punjab (2005) set stringent thresholds for criminal medical negligence under IPC Section 304A, requiring "gross negligence" beyond civil tort standards to protect doctors from frivolous prosecution. Indian courts adopted the Bolam test (from Bolam v. Friern Hospital), deeming no negligence if conduct aligns with a responsible body of medical opinion. The Bolitho addition (Bolitho v. City and Hackney HA), accepted in India, mandates courts scrutinize if such opinions withstand logical analysis.

3.3 AI and Anthropocentric Limits

Traditional frameworks like Jacob Mathew[6] and Bolam-Bolitho presume human fault, anchored in anthropocentric notions of intent, judgment, and negligence. AI involvement challenges this: autonomous systems lack agency, shifting liability to doctors (for over-reliance), hospitals, or developers via product liability or Consumer Protection Act 2019. Courts must adapt proximate causation for "black-box" errors, were algorithmic opacity obscure's fault attribution, potentially requiring new standards like algorithmic transparency mandates. Indian law lacks AI-specific

[5] Achutrao Haribhau Khodwa v. State of Maharashtra, (1996) 2 S.C.C. 634
[6] Jacob Mathew v. State of Punjab, (2005) 6 S.C.C. 1

provisions, exposing gaps in holding non-human actors accountable.

4. CONSUMER PROTECTION ACT, 2019 AND AI-MEDIATED SERVICES

Consumer Protection Act, 2019 (CPA 2019) provides a robust mechanism for addressing deficiencies in services, including those mediated by AI in healthcare. This chapter examines its application to medical services, AI diagnostics, and institutional accountability.

4.1 Healthcare as Service

Section 2(42) defines "service" broadly as any description made available to users, including but not limited to banking, insurance, transport, etc., excluding free services or personal contracts. Despite excluding explicit mention of "healthcare" (unlike draft versions), courts interpret paid medical services as falling under CPA 2019 via the *Indian Medical Association v. V.P. Shantha*[7] precedent, allowing patients as consumers to seek redress. Free services remain exempt, but mixed paid/free providers face liability for paid cases.

4.2 Deficiency in AI-Assisted Diagnosis

Deficiency under Section 2(11) encompasses faults, imperfections, or inadequacies in service quality, including negligence or withheld information causing loss. In AI-assisted diagnosis, errors like bias or miscalibration constitute deficiencies if they lead to harm, attributable to over-reliance without validation. Patients can claim compensation via Consumer Forums for faulty AI outputs, as doctors must ensure reasonable care; algorithmic opacity may evidence inadequacy.

4.3 Institutional Liability

Hospitals and clinics bear vicarious liability for staff negligence or tool deficiencies under CPA 2019's product liability provisions (Sections 82-87). As service providers deploying AI tools, institutions risk claims for "defective products" or service shortfalls, especially if unvalidated algorithms cause harm. Liability extends to developers/manufacturers if AI qualifies as a "medical device," with hospitals required to disclose risks and maintain oversight.

[7] Indian Med. Ass'n v. V.P. Shantha, (1995) 6 S.C.C. 651

Aspect	CPA 2019 Provision	AI Healthcare Implication
Service Definition	Sec 2(42): Broad, non-exhaustive list	Paid diagnostics covered; AI tools as aids
Deficiency	Sec 2(11): Faults causing loss	AI errors = negligence if unmitigated
Institutional Role	Product liability (Secs 82-87)	Hospitals liable for deployment failures

5. PRODUCT LIABILITY AND AI-ENABLED MEDICAL DEVICES

Product liability under Indian law extends to AI-enabled medical devices through the Consumer Protection Act, 2019, treating them akin to defective goods. This chapter covers Software as a Medical Device (SaMD), defect analogies, and CDSCO's regulatory oversight.

5.1 Software as Medical Device

SaMD refers to standalone software intended for medical purposes like diagnosis, prevention, monitoring, treatment, or alleviation of disease, without hardware integration[8]. AI-based SaMD uses machine learning for adaptive functions, e.g., image analysis or predictive diagnostics, classified by risk under Medical Devices Rules, 2017. In India, CDSCO recognizes SaMD if developed for clinical use, subjecting it to lifecycle regulation including validation

5.2 Product Liability Analogies

CPA 2019 Sections 82-87 impose strict liability on manufacturers for harm from defective products, covering manufacturing defects (deviations from specs), design defects (inherent flaws), and warning defects (inadequate instructions/risks). [page:0 from previous] For AI SaMD, manufacturing defects include erroneous training data; design defects arise from biased algorithms or lack of robustness; warning

[8] Med. Devices Rules, 2017, Gazette of India, Extra., G.S.R. 78(E) (Jan. 31, 2017)

defects from undisclosed limitations like drift. Plaintiffs need not prove negligence, only defect and causation.

Defect Type	Description	AI SaMD Example
Manufacturing	Aberration in production	Faulty deployment of trained model
Design	Unsafe inherent configuration	Algorithmic bias in diagnostics
Warning	Insufficient disclosures	No alerts on data drift risks

5.3 CDSCO Role

CDSCO, under Drugs & Cosmetics Act, 1940 and Medical Devices Rules, 2017, regulates AI SaMD as Class B/C/D devices based on risk (e.g., Class C for cancer diagnostics). It mandates import licenses (MD-15), clinical evaluations, QMS, post-market surveillance, and algorithm transparency for AI/ML updates. Recent 2025-2026 draft guidance clarifies SiMD vs. SaMD, aligning with global standards for lifecycle oversight. Non-compliance invites penalties, ensuring safety before market entry.

6. DATA PROTECTION, IT LAW, AND ALGORITHMIC GOVERNANCE

Digital Personal Data Protection Act, 2023 (DPDPA) and Information Technology Act, 2000 (IT Act) form the backbone of algorithmic governance in AI-health systems, protecting sensitive health data while imposing compliance duties. This chapter links data harms to negligence claims.

6.1 Health Data under DPDPA 2023

DPDPA defines "personal data" broadly, with health data as sensitive, requiring explicit consent, purpose limitation, data minimization, and security safeguards for processing[9]. Healthcare providers act as Data Fiduciaries, obligated to notify breaches to the Data Protection Board and affected individuals within timelines, appoint DPOs for large-scale processing, and enable rights like erasure. Rules emphasize encryption,

[9] Digital Personal Data Protection Act, No. 18 of 2023, §§ 4–8, 14–16, Gazette of India, Extra., pt. II-sec. 1.

audits, and retention limits for health records.

6.2 Data Harms and Negligence Interface

Data breaches cause harms like identity theft, discrimination, stigma, or emotional distress, actionable under DPDPA with fines up to ₹250 crore[10]. These intersect medical negligence where breaches exacerbate physical harm, e.g., leaked data leading to delayed treatment; victims claim compensation via tort or CPA alongside privacy remedies. Algorithmic misuse in AI-health amplifies risks, blending data violations with care deficiencies.

6.3 IT Act Security Obligations

Section 43A holds body corporates liable for negligent handling of sensitive personal data/information (SPDI)[11], including health details, mandating reasonable security practices per IT Rules 2011 (ISO 27001 compliance). AI-health systems must implement access controls, encryption, and audits; breaches trigger compensation under Section 43A or criminal penalties (Sections 66, 72). SPDI Rules require consent and non-disclosure without authorization, extending to AI training data.

`Law	**Key Provisions**	**AI-Health Application**
DPDPA 2023	Consent, breach notice, rights	Sensitive health data processing
IT Act 2000	Sec 43A negligence, SPDI Rules	Security for AI systems

8. DOCTRINAL GAPS AND THE "REGULATORY VACUUM"

8.1 Attribution of fault in multi-stakeholder AI-health ecosystems

Modern AI-health systems involve clinicians, hospitals, device/software vendors, data-providers, and sometimes cloud-and-AI-platform providers, yet traditional liability doctrines are built

[10] Ibid. Sec 33

[11] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Extra., G.S.R. 313(E)

for *single* responsible actors (e.g., a surgeon or a manufacturer).

A. Responsibility gaps and "responsibility vacuums"

- When an AI-assisted diagnostic tool blunders, it is rarely clear whether the fault lies with the clinician who over-trusted the output, the vendor who trained the model on biased data, the hospital that failed to monitor drift, or the regulator that granted clearance.
- Scholars describe this as a *responsibility gap* or *responsibility vacuum*[12]: AI systems lack legal personhood, yet multiple human actors share partial causal influence, dissipating blameworthiness.

B. Doctrinal responses needed

Current tort and product-liability regimes often rely on *proximate cause* and *duty of care* blocks that struggle to capture distributed, continuous, and iterative AI-driven failures (e.g., model drift, feedback-loop bias).

- Some proposals call for "shared wrongs" or *joint-and-several*-type liability models, or "responsibility-sharing"[13] frameworks that allocate risk across developers, deployers, and clinicians according to control, knowledge, and incentive structures.

8.2 Attribution of fault in multi-stakeholder AI-health ecosystems

Modern AI-health systems involve clinicians, hospitals, device/software vendors, data-providers, and sometimes cloud-and-AI-platform providers, yet traditional liability doctrines are built for *single* responsible actors (e.g., a surgeon or a manufacturer).

8.3 Doctrinal responses needed

- Current tort and product-liability regimes often rely on *proximate cause* and *duty of care* blocks that struggle to capture distributed, continuous, and iterative AI-driven failures (e.g., model drift, feedback-loop bias).

- Some proposals call for "shared wrongs" or *joint-and-several*-type liability models, or "responsibility-sharing" frameworks that allocate risk across developers, deployers, and clinicians according to control, knowledge, and incentive structures.

[12] John Danaher, The Threat of Algocracy: Reality, Resistance and Accommodation, 29 Phil. & Tech. 245, 253–60 (2016)
[13] Andrea Bertolini, Artificial Intelligence and Civil Liability, in *Research Handbook on AI and Law* 505, 512–18 (Woodrow Barfield & Ugo Pagallo eds., 2020)

8.4 Black-box problem and evidentiary burden

Most AI-based medical tools act as "black boxes" (in particular deep learning models), which makes it difficult to piece together why a particular decision was reached, and in turn who (or what) deviated from the standard of care.

8.5 Transparency and explainability deficits

Even where regulators impose requirements for "interpretability" or "explainability" (such as those in the EU AI Act's high risk system rules), the technical and legal standards are vague and many of the proprietary models remain opaque to both clinicians and the courts. This opacity directly undermines disclosure duties (e.g., informing patients about AI assisted decisions) and informed consent, as the "how" and "how reliable" cannot be clearly communicated.

8.6 Definitions and classification gaps

Laws often lack clear definitions of "AI-medical device," "AI-clinical decision support," or "autonomous AI agent," forcing regulators to squeeze AI tools into existing device, software, or liability categories whose thresholds do not fit well. Without precise typologies, it becomes difficult to calibrate risk-based regimes (e.g., high-risk vs low-risk SaMD/AI-MD) consistently across jurisdictions. lack of harmonised standards and reporting:

- Although WHO and others propose governance and ethics frameworks, there is no globally harmonised set of technical standards (e.g., on data quality, bias-bias-mitigation, or robustness testing) that bind courts or regulators.

- Reporting mechanisms for AI-related adverse events are often fragmented: many AI-driven decisions fall outside classic medical-device-vigilance systems, creating a *regulatory vacuum* between device-law and general tort-law.

9. PROPOSED FRAMEWORK FOR INDIA

9.1 Need for a defined "AI-medical system" category

- A dedicated statutory definition of "AI-assisted healthcare system" (analogous to FDA SaMD or EU AI-Act high-risk categories) would clarify what falls under special oversight, particularly for diagnostic, prognostic, and therapeutic

decision-support tools.[14]

- This definition should distinguish between fully automated mechanisms (e.g., triage or screening bots) and human in the loop decision support tools to calibrate regulatory intensity.

9.2 Regulatory anchoring

- The framework could sit at the intersection of the Drugs and Cosmetics Act / Medical Devices Rules, the Telemedicine Guidelines, and a future AI-in-Health Act or substantial amendment to the Digital Information Security in Healthcare Act (DISHA-style) legislation.

- Statutory recognition would enable tailored requirements for pre validation, ongoing monitoring, and sunset clauses for models that fall below performance thresholds.[15]

9.3 Suggested amendments/themes to integrate AI-error into India's medico-legal framework

- To operationalize this framework, you can propose several doctrinal and legislative themes that amend or reinterpret existing Indian law:

9.4 Amendments to the Indian Medical Council / NMC regime

- Introduce AI-competency standards for clinicians and hospitals, requiring basic training in AI-tool limitations, bias awareness, and human-supervision protocols as part of continuing medical education and accreditation.

- Clarify that over-reliance on AI or failure to verify AI outputs may constitute professional misconduct, subject to disciplinary action under the National Medical Commission framework.

9.5 Integration into tort and consumer protection law

- Read the Consumer Protection Act, 2019 and tort law doctrines of negligence to recognize AI assisted decisions as services that can be defective by design or deployment, not just by human error.

- Courts could develop a "reasonableness of AI use" standard,

[14] U.S. Food & Drug Admin., Software as a Medical Device (SaMD): Clinical Evaluation (2017)
[15] WHO, Ethics and Governance of Artificial Intelligence for Health (2021),

analogous to the Bolam test, but calibrated to:

a. adequacy of AI tool validation,

b. presence of appropriate safeguards, and

c. clinician training level.

9.6 Legislative "AI in Health" chapters

- A future central law or substantial amendment to the National Digital Health Mission framework could contain a dedicated chapter on AI in health, specifying:

- Definitions of AI medical systems and AI assisted decision support.

- Risk based classification (e.g., low risk administrative tools vs high risk diagnostic tools).

- Mandatory transparency, audit trail, and reporting obligations, with penalties for non-compliance.

10. CONCLUSION

Balancing innovation, accountability, and patient safety

In closing, the central challenge is not to *stop* AI-health innovation, but to embed accountability and safety into its design and deployment so that the benefits of early-diagnosis, resource-optimisation, and remote-care can be realised without sacrificing patient-trust or legal redressibility.

- Innovation must be nurtured through predictable, risk-proportionate rules that distinguish between high-risk AI-diagnostic tools and low-risk administrative or triage aids, avoiding blanket stifling of experimentation.

- Accountability requires closing the doctrinal gaps: tiered liability, clear transparency and logging obligations, and workable AI specific evidentiary pathways ensure that those who cause harm—whether clinicians, vendors, or institutions—can be identified and held responsible.

Patient safety benefits from a dual strategy: strong ex-ante regulatory checks (pre-validation, vigilance, and drift-monitoring) paired with robust ex-post mechanisms (adverse-event reporting, audits, and

credible tort-law remedies).