Advances in Consumer Research
https://acr-journal.com/
Volume-2 | Issue-5 | October 2025
Original Researcher Article

The Intersection of Law, Ethics, and Healthcare Ai: Policy Pathways for Responsible Innovation

Dr Gagandeep Kaur[1] and Dr Vinod Kumar Shukla[2]

[1]Senior Associate Professor in Law, School of Law, UPES,
Email: gkaur@ddn.upes.ac.in
[2]Associate Professor, Amity University, Dubai,
Email: vshukla@amityuniversity.ae

Received: 02/10/2025
Revised: 10/10/2025
Accepted: 28/10/2025
Published: 29/10/2025

ABSTRACT
Artificial intelligence in health systems has moved from experimental pilots to regulated products and routine clinical workflows. The resulting entanglement of machine learning with diagnosis, triage, imaging, therapeutics, and public health surveillance raises legal and ethical questions that cannot be answered within any single doctrinal silo. This paper examines the intersection of law and ethics in healthcare AI through four moves. First, it distils the scholarly literature on core risks and remedies: privacy, consent, bias and distributive justice, explainability and accountability, safety and post-market learning, cybersecurity, and the governance of adaptive models. Second, it maps the evolving regulatory landscape across jurisdictions with attention to instruments that now structure deployment: the European Union's risk-based AI Act and the Medical Device Regulation, the United States Food and Drug Administration's approach to software as a medical device and Predetermined Change Control Plans, the World Health Organization's guidance on ethics and governance for both conventional AI and large multimodal models, and India's emergent framework combining the Digital Personal Data Protection Act 2023, the Medical Device Rules 2017, Telemedicine Practice Guidelines 2020, and the Ayushman Bharat Digital Mission's Health Data Management framework. Third, it situates Indian constitutional doctrine and health jurisprudence as normative anchors for responsible innovation, showing how privacy, autonomy, dignity, and the right to health cohere into constraints on design and deployment. Finally, it proposes concrete policy pathways for regulators, hospitals, payers, and developers: regulatory sandboxes and staged evidence, algorithmic impact assessments, data-protection by design and federated approaches, auditability and safety cases, procurement-driven standards, professional duties for AI-assisted care, arrangements for accountability and insurance, and participatory oversight. In doing so, the paper argues for a principled and practicable equilibrium between innovation and fundamental rights that is attentive to Indian realities yet interoperable with global regimes (WHO; EU; FDA).

Keywords: Healthcare AI; data protection; algorithmic accountability; software as a medical device; explainable AI; federated learning.

INTRODUCTION:

Clinical AI is no longer a research novelty. Imaging classifiers triage scans before radiologists open their worklists; predictive models flag sepsis and readmission risk; conversational agents assist triage and counselling; and hospital operations use forecasting to allocate beds and staff. These capabilities increase scale, speed, and sensitivity, yet they also externalise risk across patients, professionals, and institutions. If law lags, harms are normalised and trust erodes. If law over-corrects, beneficial systems are chilled. The central problem is to calibrate governance to the specific failure modes of learning systems without dissolving the clinical virtues of prudence, deliberation, and accountability.

Internationally, a regulatory architecture has begun to coalesce. The European Union's AI Act adopts a risk-based regime that classifies many health applications as "high-risk" with attendant conformity assessment and post-market duties, building on device regulation under the Medical Device Regulation 2017/745. The United States has incrementally shaped oversight for software as a medical device, including an approach to adaptive models through Predetermined Change Control Plans. The World Health Organization has framed ethics and governance principles and, in 2024–2025, issued guidance tailored to large multimodal models in health. India is assembling a layered framework of personal data protection, medical device regulation, telemedicine, and a national digital health stack, with constitutional jurisprudence on privacy, autonomy, and the right to health providing substantive constraints and direction. Together these developments create both normative and practical baselines for responsible innovation.

REVIEW OF LITERATURE

Scholarly analysis of healthcare AI concentrates on recurrent concerns and corresponding governance strategies.

1. Bias, fairness, and distributive justice. Empirical and review studies show that AI systems trained on skewed datasets can underperform for under-represented populations, perpetuate clinical disparities, and misallocate resources. Reviews in Journal of Biomedical Informatics and EClinicalMedicine catalogue mitigation methods, from re-sampling to counterfactual fairness, while emphasising the institutional and data-generating causes of bias (Carey, 2024; Yang et al., 2024). These literatures argue for measurement parity, subgroup reporting, and continuous post-deployment monitoring.
2. Explainability and accountability. Systematic reviews across ScienceDirect titles detail the state of explainable AI in clinical imaging and decision support, highlighting trade-offs between performance and interpretability and the need to validate explanations with clinicians and patients (Muhammad et al., 2024; Sadeghi et al., 2024; Band et al., 2023). The consensus is that explainability is a means to safety and accountability rather than an end in itself and must be integrated with documentation, calibration and uncertainty reporting.
3. Privacy-preserving learning. Surveys of federated learning in medicine argue that cross-institutional model training without centralising patient data can advance performance and generalisability while aligning with data-protection obligations, albeit with new attack surfaces that require secure aggregation, differential privacy and governance agreements (Zhang et al., 2024; Xu et al., 2020/2021).
4. Trust, safety, and LMMs. WHO's guidance synthesises ethical risks for both conventional AI and large multimodal models, recommending governance architectures that centre human oversight, transparency, accountability, and equity, including controls for hallucinations, provenance, and model updates.
5. Regulatory scholarship. Commentaries note the convergence of device regulation, data protection, and administrative oversight. Recent analyses of the EU AI Act's interaction with medical device law emphasise combined obligations for design, quality management, and post-market surveillance. FDA materials explain how adaptive models may be pre-specified within change plans, shifting some regulatory scrutiny upstream (to the plan) and downstream (to real-world monitoring).

Background of Study

The technology and its failure modes: Healthcare AI encompasses supervised and self-supervised learning, reinforcement learning in clinical pathways, and generative models for text, images, and multimodal records. Typical risks include distributional shift, spurious correlations, overfitting to hospital-specific practice patterns, and automation bias among clinicians. LMMs raise specific concerns regarding provenance, hallucination, and leakage of sensitive prompts and outputs, which complicate consent and secondary use.

Global governance baselines: Three regimes are especially formative. First, the EU AI Act imposes pre-market conformity assessment, quality management systems, technical documentation, data and data-governance duties, transparency obligations, human oversight measures, and post-market monitoring for high-risk systems. Health applications that are themselves medical devices must comply with both the AI Act and the Medical Device Regulation. Second, the US FDA treats clinical AI predominantly as software as a medical device. The Agency's approach to adaptive systems uses Predetermined Change Control Plans that pre-specify the model elements subject to change, the methods for change, and performance limits; these plans are reviewed at clearance and then governed through real-world performance monitoring. Third, WHO articulates six ethical principles and, most recently, guidance for LMMs in health with more than forty recommendations for governments, developers, and providers, including evaluation standards, documentation, and public communication.

India's digital-health context: India's Digital Personal Data Protection Act 2023 establishes consent, purpose limitation, duties for significant data fiduciaries, a Data Protection Board, and penalties. The Medical Device Rules 2017 under the Drugs and Cosmetics Act brought a risk-based classification aligned with global practice and have been interpreted to encompass software as a medical device. The Telemedicine Practice Guidelines 2020 regularised remote care and clarified professional responsibilities. The Ayushman Bharat Digital Mission and Health Data Management Policy create a federated digital health ecosystem with consent-mediated data sharing and interoperability through public digital infrastructure. These instruments provide a scaffold for lawful, ethical AI deployment with strong interactions between device law and data protection.

An Analysis of Legal Challenges

1) Data protection, consent, and secondary use

Healthcare AI requires large, diverse datasets. The DPDP Act's lawful grounds, notice and consent, age-assurance for children, and significant data fiduciary obligations require developers and hospitals to define purposes, minimise data, and log processing. Secondary uses such as model improvement and domain adaptation demand granular consent or another lawful ground and a clear separation of roles among controllers, processors, and consent managers within the ABDM ecosystem. Cross-border model development triggers transfer conditions. Parallel EU law treats health data as a special

category with safeguards, while limiting automated decision-making with legal or similarly significant effects.

2) Safety, effectiveness, and post-market learning

Clinical AI that qualifies as a medical device must satisfy safety and performance requirements, supported by technical documentation and clinical evidence. Adaptive models introduce "learning after deployment," requiring change control, periodic performance review, and real-world evidence. The FDA's PCCP model and the EU Act's post-market monitoring illustrate convergent strategies that India can adapt within MDR 2017 and CDSCO guidance.

3) Bias, discrimination, and equality before law

Bias mitigation is a legal as well as an ethical duty. Discriminatory impacts may offend constitutional guarantees and anti-discrimination statutes when AI systematically disadvantages protected groups. Mitigations include balanced sampling, subgroup performance metrics, documented data lineage, and routine bias audits embedded in quality-management systems. Literature emphasises that mere technical fixes are insufficient without governance and accountability. (ScienceDirect)

4) Explainability, documentation, and professional accountability

Where AI materially shapes diagnosis or treatment, clinicians remain answerable for decisions. Explainability supports the duty to give reasons and the patient's informed consent. Reviews caution that explanations must be calibrated to clinical utility and validated, not adopted as a veneer over unreliable models. Hospitals should require "model facts labels," uncertainty bounds, failure-mode documentation, and audit logs to support ex post explanations in complaint or litigation (Carey, 2024).

5) Cybersecurity and model integrity

Compromised models endanger patients. Security standards must address data pipelines, model updates, adversarial manipulation, poisoning, and inference attacks. Federated learning mitigates centralised aggregation risks but introduces new vulnerabilities at the client and aggregator level, requiring secure aggregation, attestation, and incident response.

6) Liability and redress

When harm occurs, causal chains are complex. Possible defendants include manufacturers, deployers, and professionals. Product liability must adapt to data-dependent performance and updates; negligence must revisit the standard of care for AI-assisted decisions; and hospitals should align clinical governance with duty to monitor deployed systems. Arrangements for insurance and indemnities are needed in procurement and licensing.

7) Intellectual property, trade secrets, and transparency

Regulators and hospitals need enough visibility to evaluate safety and fairness. Trade secret claims cannot defeat audit, safety cases, or public accountability where fundamental rights are implicated. Structured transparency, including access to documentation, model cards, and evaluation data under confidentiality, reconciles innovation with oversight.

LANDMARK CASE LAWS IN INDIA

Indian constitutional and health jurisprudence offers first-principles for AI governance.

1. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) recognised privacy as a fundamental right and articulated proportionality and necessity tests for state action. Any health-AI deployment by public authorities or mandates upon private entities must satisfy these tests, including legitimate aim, rational connection, minimal impairment, and balancing.
2. Justice K.S. Puttaswamy v. Union of India (Aadhaar) (2018) refined proportionality in data-intensive schemes, underscoring purpose limitation and safeguards. This is salient for ABDM-linked AI that relies on identity-linked records.
3. Selvi v. State of Karnataka (2010) prohibited involuntary narco-analysis and similar techniques, grounding a strong conception of bodily and mental autonomy. The reasoning speaks against coercive data extraction and opaque inferences about mental states.
4. Suchita Srivastava v. Chandigarh Administration (2009) protected decisional privacy and reproductive autonomy, implying robust consent standards for AI in reproductive health and counselling.
5. Common Cause v. Union of India (2018) affirmed the right to die with dignity and recognised advance directives, reinforcing the requirement that AI-mediated care respect patient preferences and informed choices.
6. Parmanand Katara v. Union of India (1989) and Paschim Banga Khet Mazdoor Samity v. State of West Bengal (1996) established obligations to provide timely emergency care and to organise health systems to meet that duty, relevant to triage algorithms and resource allocation tools.
7. Mr. X v. Hospital Z (1998) balanced medical confidentiality with public health interests, illustrating how privacy yields in limited circumstances under law and due process.

Case (Year; Citation)	Core issue	Holding / principle	Relevance to healthcare AI	Compliance actions for deployers and clinicians
Justice K.S. Puttaswamy (Retd.) v. Union of India (2017; (2017) 10 SCC 1)	Whether privacy is a fundamental right and the test for limits on data-intensive state action	Privacy held to be a fundamental right under Articles 14, 19, and 21. Any infringement must meet the four-part proportionality test: legitimate aim, rational connection, necessity, and balancing	Any government use or mandate of clinical AI, data lakes, or population models must satisfy proportionality. Bulk health-data processing without tight purpose limitation is constitutionally suspect	Conduct documented proportionality analysis; adopt purpose limitation and data minimisation; maintain audit trails; enable rights to notice, access, and grievance
Puttaswamy (Aadhaar) (2018; (2018) 1 SCC 809)	Constitutional limits on identity-linked data ecosystems	Reaffirmed proportionality. Stressed purpose limitation, necessity, and robust safeguards for identity-linked processing	National digital health systems that link longitudinal records to unique IDs must show strict necessity and safeguards when used to train or deploy AI	Separate identifiers from model training data where possible; use tokenisation; publish data-protection impact assessments; restrict secondary use
Selvi v. State of Karnataka (2010; (2010) 7 SCC 263)	Involuntary narco-analysis and related techniques	Non-consensual extraction of information violates personal liberty and mental privacy	Prohibits coercive data extraction and inference about mental states without informed consent. Relevant to AI that predicts cognition, mood, or competence	Obtain explicit, specific consent for mental-state inference; provide opt-out; avoid covert psychometric profiling
Suchita Srivastava v. Chandigarh Administration (2009; (2009) 9 SCC 1)	Reproductive autonomy and decisional privacy	Recognised reproductive autonomy as an aspect of personal liberty and privacy	AI tools in reproductive health, counselling, and fertility must respect decisional autonomy and avoid nudging beyond informed choice	Strengthen informed consent with risk, limitation, and alternatives; ensure clinician-supervised use; log recommendations and overrides
Common Cause v. Union of India (2018; (2018) 5 SCC 1)	Right to die with dignity; advance directives	Validated advance directives and patient autonomy at end of life	Clinical decision-support for intensive care, triage, or escalation must incorporate patient preferences and advance directives	Integrate directive status into AI inputs; surface patient-preference flags; require human confirmation before irreversible steps
Parmanand Katara v. Union of India (1989; 1989 AIR 2039)	Duty to provide immediate emergency care	Recognised an obligation to render timely medical aid	Triage and emergency-room AI must prioritise timely care and cannot justify delay due to algorithmic uncertainty	Configure AI to err toward life-saving escalation; monitor time-to-intervention metrics; set clear override rules
Paschim Banga Khet Mazdoor Samity v. State of West Bengal	State obligation to organise healthcare services	State must arrange adequate medical facilities and referral systems	Supports state deployment of AI for capacity planning and referrals, subject	Use AI for equitable resource allocation; publish fairness metrics; ensure safe

Case (Year; Citation)	Core issue	Holding / principle	Relevance to healthcare AI	Compliance actions for deployers and clinicians
(1996; (1996) 4 SCC 37)			to privacy and equity safeguards	referral logic with human oversight
Mr. X v. Hospital Z (1998; (1998) 8 SCC 296)	Medical confidentiality vs public interest	Patient confidentiality is vital but may yield to compelling public health interests	Guides disclosure rules for AI systems that detect communicable threats. Any disclosure must be lawful, necessary, and proportionate	Implement tiered disclosure policies, strict access controls, and incident documentation; perform necessity tests before disclosure

These decisions collectively insist that healthcare AI be lawful, necessary, proportionate, rights-respecting, and overseen by accountable human agents.

Legislative Provisions

1) India

1.1 Digital Personal Data Protection Act, 2023 (DPDPA)

Scope and lawful bases. The DPDPA governs processing of "digital personal data," including data first collected offline and later digitised, with extraterritorial reach when goods or services are offered to individuals in India. Processing must rest on consent or on "certain legitimate uses." Controllers are "Data Fiduciaries," individuals are "Data Principals." Consent requires a clear notice and must be as easy to withdraw as to give. Children's data receive heightened protection. Rights include access, correction, erasure, grievance redress, and nomination. Cross-border transfers are permitted by default except to countries placed on a negative list by the Central Government. Significant Data Fiduciaries must appoint a DPO, conduct periodic DPIAs and independent audits. Penalties are set out in a schedule with high statutory maxima. The Act stipulates that Section 43A of the IT Act 2000 will be omitted upon DPDPA commencement. As of today, the Act has been enacted, but key provisions depend on government notification and rules; the government has publicly indicated rules are expected by 28 September 2025. (Digital Personal Data Protection Act, ss. 1–13, 18, 44; Government announcement on rules timeline.)

Implications for healthcare AI. Hospitals, health-tech firms and SaMD vendors that process identifiable health data will be Data Fiduciaries. A DPIA will be mandatory for entities notified as "significant." Mechanisms for granular consent and withdrawal are central. Children's profiles, clinical images and sensor streams must be processed with parental consent and child-specific safeguards. Data sharing via health exchanges will require documented consent artefacts and auditable logs. Cross-border model training or cloud inference must track the negative list once notified.
Transitional note. Until full commencement, legacy obligations under the IT Act and sectoral directions continue to apply in practice, especially incident reporting to CERT-In. DPDPA section 44 provides that IT Act section 43A stands omitted only upon notification, which underscores the need to maintain IT Act–based security controls during the transition (MeitY)

1.2 CERT-In Directions, 28 April 2022

Six-hour breach reporting. Any "service provider, intermediary, data centre, body corporate or Government organisation" must report specified cyber incidents to CERT-In within 6 hours of noticing or being notified. FAQs clarify that partial information may be filed initially, with follow-up details later. Healthcare operators using networked devices, PACS, or cloud EHRs fall within the frame when they are body corporates or service providers. Maintain contact-point details, synchronised clocks, log retention, and incident runbooks aligned to the Directions.

1.3 Ayushman Bharat Digital Mission (ABDM) & Health Data Management Policy (2022)

ABDM establishes a federated, standards-based digital health infrastructure built around the ABHA number, Health Facility and Professional registries, and the Unified Health Interface. The Health Data Management Policy sets consent, purpose limitation and security expectations for ecosystem participants that integrate with ABDM rails. For AI systems consuming ABDM-linked data, maintain conformance with ABDM's consent artefacts and privacy safeguards, including encryption at rest and in transit.

1.4 Telemedicine Practice Guidelines, 2020

Notified as an Appendix to the professional conduct rules, these Guidelines authorise Registered Medical Practitioners to provide tele-consultations subject to consent documentation, identity verification, record-keeping and prescribing limits. Certain drug lists are restricted for text-only consults and for tele-prescription. Healthcare AI decision-support used in teleconsults must fit within these norms, including documentation of advice, disclosure to patients, and escalation to in-person care when indicated.

1.5 Medical Device Rules, 2017 (as amended) and SaMD

India regulates medical devices under the Medical Device Rules, 2017, administered by CDSCO. Classification by risk (Classes A–D) determines the conformity route. Software can be a medical device when intended for diagnosis, prevention, monitoring, treatment or alleviation of disease; SaMD follows the device licensing framework, quality system requirements and post-market vigilance. Recent regulator commentary and industry guidance explain risk-based classification and licensing pathways for SaMD. Clinical investigations align with the New Drugs and Clinical Trials Rules, 2019 when applicable. Developers of AI-SaMD should prepare technical files, clinical evaluation, cybersecurity documentation, and a post-market surveillance plan.

1.6 Evidence law for digital records: Bharatiya Sakshya Adhiniyam, 2023

The BSA 2023 replaces the Indian Evidence Act. It recognises electronic and digital records as documents and provides specific presumptions for electronic messages and for electronic records that are five years old. This is directly relevant to AI system logs, audit trails, and model-change records that may be relied upon in litigation or regulatory inquiries. Maintain hash-based integrity, time-stamped logs and authenticated signatures to take advantage of these evidentiary presumptions.

2) European Union

2.1 EU AI Act, 2024

Status and phased application. The AI Act entered into force on 1 August 2024, with staged applicability: prohibitions and AI literacy duties apply from 2 February 2025; governance rules and obligations for general-purpose AI models apply from 2 August 2025; most other obligations, including high-risk systems, apply from 2 August 2026, with a longer runway until 2 August 2027 where AI is embedded in products regulated under sectoral law.

Healthcare AI as "high-risk." AI that is a medical device under the MDR or IVDR is high-risk by default. Obligations include a quality management system, risk and data-governance controls, technical documentation, logging, transparency to users, human oversight and post-market monitoring. Deployers such as hospitals also have duties regarding AI literacy, usage instructions, and monitoring in clinical workflows. Coordination clauses align the AI Act with the MDR so that conformity assessment can be integrated where possible (van Kolfschooten, H., et al. (2024).

2.2 GDPR interface

Health data are "special categories" under Article 9 GDPR and require an Article 9(2) condition such as explicit consent, public interest in public health, or scientific research safeguards. Automated decision-making protections in Article 22 may be engaged where AI decisions have legal or similarly significant effects. These GDPR bases and safeguards must be engineered into datasets and deployment.

2.3 MDR, 2017/745

Software intended for medical purposes is a device under the MDR; classification rules and general safety and performance requirements apply. Notified-body assessment, post-market surveillance and vigilance obligations are central. Cybersecurity and lifecycle documentation are increasingly expected, often by reference to harmonised or state-of-the-art standards.

3) United States

The FDA regulates AI as part of device software functions when intended for medical purposes. It has issued a suite of guidances:

- Predetermined Change Control Plans (PCCPs). Final guidance sets expectations for planned post-market model modifications within an authorised change protocol. Sponsors should specify the scope of changes, data management, retraining triggers, re-validation, and updated labelling.
- AI-enabled device software functions lifecycle and submissions. Draft guidance consolidates content expectations across the device lifecycle, including risk management, dataset representativeness, training-validation-test separation, and performance monitoring.
- Good Machine Learning Practice (GMLP). Joint principles with Health Canada and MHRA cover data quality, model design, human factors, and post-deployment monitoring.

These frameworks influence global practice even outside the U.S., particularly for multijurisdictional SaMD portfolios.

4) International and Soft-law Guidance

WHO, Ethics and Governance of AI for Health and the 2025 guidance on large multimodal models articulate risk classifications, documentation, transparency to users, and monitoring obligations. They are widely referenced by regulators and health systems for policy design and vendor due diligence. Aligning institutional policies with these guidance points supports legal defensibility under multiple regimes.

5) Recognised Standards to Operationalise Legal Duties

While not legislation, these standards are frequently invoked by regulators and notified bodies to evidence conformity:

- IEC 81001-5-1:2021 on secure software life-cycle processes for health software and health IT systems. Often read alongside IEC 62304 and IEC 82304-1 and referenced for MDR conformity and EU market access. ISO+1
- IEEE 7001-2021 on transparency of autonomous systems, useful to operationalise AI Act transparency and healthcare disclosure duties. IEEE Standards Association+1

6) Practical Compliance Blueprint for Healthcare AI in India

1. Map processing under DPDPA. Identify roles as Data Fiduciary or Processor, prepare consent notices, withdrawal flows, and Data Principal rights handling. For high-risk processing, anticipate Significant Data Fiduciary designation and stand up DPIA and independent audit capacity. Track cross-border data flows pending the negative-list notification. MeitY
2. Prepare for CERT-In. Build a six-hour incident reporting playbook, designate a Point of Contact, test log aggregation and time-sync, and retain logs for the periods prescribed. CERT-IN
3. Align with ABDM. If integrating with ABDM rails, implement consent artefacts and data-minimisation controls per the Health Data Management Policy; validate encryption and DLP controls. World Bank
4. Telemedicine workflows. Ensure AI decision-support used in virtual care respects the Telemedicine Guidelines on consent, documentation and prescribing limits. Update SOPs and patient information leaflets accordingly. PubMed Central
5. Device regulation. Decide whether your software is SaMD. If yes, classify by risk, implement QMS, clinical evaluation, cybersecurity per IEC 81001-5-1, and vigilance. Prepare for CDSCO licensing and for NDCT rules if clinical investigations are planned. EUR-Lex+1
6. Evidence readiness. Preserve model lineage, training data provenance, PCCPs where applicable, and change logs with cryptographic integrity. This supports BSA presumptions for electronic records and reduces evidentiary disputes. Ministry of Home Affairs

Jurisdiction / Instrument	Scope & Coverage	Key Obligations	Current Status / Timeline	Implications for Healthcare AI
India – Digital Personal Data Protection Act, 2023 (DPDPA)	Applies to all processing of digital personal data; extraterritorial reach	Consent or "certain legitimate uses"; rights to access, correction, erasure; duties of Data Fiduciaries; DPIAs and audits for Significant Data Fiduciaries; cross-border transfers subject to negative list	Enacted; rules to operationalise expected by Sept 2025; Sec. 43A IT Act to be omitted upon notification	Hospitals, SaMD vendors, telehealth platforms must implement consent artefacts, rights-handling, breach logs, and lawful bases. Cross-border AI model training contingent on transfer rules
India – CERT-In Directions, 2022	All service providers, intermediaries, data centres, body corporates	Six-hour reporting of specified cyber incidents; synchronised clocks; log retention (180 days); contact-point details	Binding from June 2022	Health AI operators must maintain incident response playbooks; critical for medical imaging PACS, EHR systems and AI cloud services
India – ABDM & Health Data Management Policy (2022)	National digital health stack (ABHA IDs, registries, consent managers)	Consent-mediated data sharing; purpose limitation; security requirements; interoperability	Live, phased enrolment of facilities and professionals	AI consuming ABDM-linked data must conform to consent artefacts and encryption standards
India – Telemedicine Practice Guidelines, 2020	Teleconsultations by Registered Medical Practitioners	Consent, identity verification, documentation, prescribing limits	In force as appendix to professional conduct rules	AI used in teleconsults must disclose its role, support doctor's duty to record, and avoid prescribing beyond allowed lists
India – Medical Device Rules, 2017 (MDR)	Medical devices, incl. software with medical purpose	Risk-based classification (A–D), licensing, QMS, clinical evaluation,	In force; amendments ongoing; CDSCO licensing required	AI-SaMD must be licensed, with technical files, cybersecurity documentation, and PMS systems

Jurisdiction / Instrument	Scope & Coverage	Key Obligations	Current Status / Timeline	Implications for Healthcare AI
		post-market surveillance		
India – Bharatiya Sakshya Adhiniyam, 2023 (BSA)	Evidence law replacing Indian Evidence Act	Digital records recognised; presumptions for electronic messages and records ≥5 years	In force (effective July 2024)	Hospitals and AI vendors should maintain integrity-protected logs, signatures, and timestamps for evidentiary admissibility
EU – AI Act, 2024	AI systems; high-risk category includes health/medical	QMS, data governance, transparency, documentation, human oversight, post-market monitoring	Entered into force Aug 2024; main duties effective Aug 2026; longer runway until 2027 for embedded devices	Any AI deployed in EU hospitals must satisfy high-risk conformity and MDR alignment; deployers (hospitals) also have monitoring duties
EU – GDPR (2016)	Personal data processing, special categories incl. health data	Article 9: explicit consent or other lawful basis; Article 22: restrictions on automated decisions	In force since 2018	Training and deployment of health AI must embed explicit consent or safeguards; Article 22 triggered if decisions are legally/significantly impactful
EU – MDR, 2017/745	Medical devices incl. SaMD	Clinical evaluation, risk management, PMS, notified body review	In force May 2021	AI intended for diagnosis/treatment is regulated as a device; strict lifecycle controls apply
USA – FDA SaMD Framework	Software as a medical device	PCCPs (pre-specified change plans); Good ML Practices; real-world monitoring	PCCP guidance finalised 2024; lifecycle draft guidance issued	Developers must specify update protocols, performance limits, validation, and labelling; global vendors follow FDA playbooks
International – WHO Guidance (2021; 2025)	AI in health; large multimodal models	Ethics and governance principles; >40 recs on transparency, evaluation, oversight	2021 guidance (AI in health); 2025 LMM guidance	Provides global benchmarks; hospitals and governments adopt for trust and accountability
Standards (IEC 81001-5-1; IEEE 7001, 7002, 7010)	Secure lifecycle processes; transparency; privacy processes; well-being metrics	Integrates into QMS and procurement	Voluntary but referenced by regulators and procurers	Used to evidence compliance with MDR, AI Act, or DPDPA; provides operational scaffolding

Legal Challenges, Revisited as Doctrinal Questions

1. Is AI-assisted care consistent with informed consent? Yes, provided consent processes disclose AI involvement in a clinically meaningful way, including limits, uncertainties, and human oversight. Where AI is invisible to patients, transparency and documentation support consent and subsequent redress.
2. What standard of care governs clinicians using AI? The prudential standard remains the reasonably competent practitioner with access to such tools, not the tool itself. However, standard-setting bodies and professional councils should articulate when reliance on AI is prudent or negligent, including double-checking thresholds and overrides.
3. Who is responsible when models update? Manufacturers bear duties to validate updates within approved change plans; deployers bear duties to monitor; clinicians must attend to out-of-distribution warnings and override options. Contracts must allocate responsibilities for surveillance, incident response, and recalls.
4. How do courts assess bias claims? Plaintiffs can challenge discriminatory impacts under constitutional equality and statutory frameworks; defendants must show necessity and proportionality and demonstrate effective risk management and mitigation.

Policy Pathways for Responsible Innovation

1. Algorithmic Impact Assessments (AIAs) and Data Protection Impact Assessments (DPIAs). Require pre-deployment AIAs integrated with DPIAs for significant deployments, addressing purpose, data lineage, lawful basis, affected rights, bias risks, update pathways, and redress arrangements (DPDP Act; GDPR practice). (PRS Legislative Research)
2. Regulatory sandboxes and staged evidence. Use time-limited, scope-limited trials overseen by CDSCO and state health authorities to collect real-world evidence, especially for adaptive or LMM-based tools, with mandatory public protocols.
3. Pre-specification via PDPs/PCCPs. For adaptive models, require pre-approved change plans specifying the learning algorithm, boundaries for performance drift, datasets permitted for updates, and triggers for re-review, drawing on FDA practice. (U.S. Food and Drug Administration)
4. Federated and privacy-preserving data pipelines. Incentivise multi-institution training through federated learning with secure aggregation, differential privacy, and governance agreements, thereby reducing data transfer risks while improving model generalisability. (ScienceDirect)
5. Equity-by-design. Mandate subgroup performance reporting, bias testing, and mitigation before approval and as a condition of continued use, with corrective action plans and sunset clauses for persistently inequitable tools. (ScienceDirect)
6. Explainability and documentation requirements. Require model facts labels, intended use, contraindications, uncertainty measures, human-oversight instructions, and change logs; link explainability to clinical tasks rather than abstract transparency.
7. Safety cases and audit trails. Borrow from high-reliability industries and require developers to maintain structured safety cases that assemble evidence for claims about safety and performance, paired with immutable audit logs for forensic review.
8. Procurement as governance. Hospitals and public payers should use contracts to impose IEEE-aligned privacy processes (IEEE 7002) and well-being impact assessments (IEEE 7010), bias testing, audit rights, service-level security, update governance, and indemnities.
9. Professional guidance. The National Medical Commission and specialty bodies should issue practice advisories on appropriate reliance, documentation, patient communication, and override duties for AI-assisted care, aligned with telemedicine norms.
10. Accountability and insurance. Clarify liability allocation among manufacturers, integrators, and providers; require insurance and risk-pooling mechanisms reflecting AI-specific hazards.
11. Public communication and explainers. Following WHO guidance, publish plain-language summaries for material deployments, including known risks and evidence levels, to maintain legitimacy and trust.
12. Independent oversight and appeals. Establish institutional ethics-technology committees with patient representation to review high-impact deployments and to hear patient complaints and appeals concerning AI-mediated decisions.

CONCLUSION

Healthcare AI can enlarge clinical capacities and make systems more just by reducing unwarranted variation and increasing access. It can also harm by magnifying bias, masking error with spurious certainty, and eroding confidentiality. Institutions therefore need law that is not simply restrictive but enabling with conditions: it should insist on purpose clarity, data stewardship, human oversight, equity, safety, and accountability, while giving innovators predictable pathways to approval, adaptation, and scale. The trajectories of the EU AI Act, FDA change-control planning, WHO ethical guidance, and India's data-protection and device regimes are converging on such a conditional permission structure. The normative commitments of Indian constitutional law supply firm guardrails. The policy pathways proposed to translate those commitments into operational governance for developers, hospitals, and regulators alike.

Suggestions

1. Enact subordinate legislation and guidance under the DPDP Act tailored to health AI, clarifying lawful bases for secondary use, research exemptions, children's data, and cross-border model development. (PRS Legislative Research)
2. Issue CDSCO guidance that explicitly operationalises SaMD classification for AI, including adaptive models, with templates for change-control plans, post-market monitoring, and bias reporting; coordinate with the National Medical Commission on clinical responsibilities. (CDSCO)
3. Adopt a national AIA template for healthcare deployments, integrated with ABDM consent flows and registries, and require publication of non-confidential summaries. (PubMed Central)
4. Create a public registry of AI tools deployed in hospitals, including evidence summaries, known limitations, subgroup performance, and recall history.
5. Establish a multi-stakeholder Health AI Sandboxing Programme to evaluate LMM-based tools in controlled settings with clear exit criteria and public reports, drawing on WHO's recommendations for transparency and oversight. (World Health Organization)

6. Use public procurement to require IEEE 7002 privacy processes and IEEE 7010 well-being assessments, together with security, auditability, and incident response covenants. (IEEE Standards Association)
7. Mandate federated and privacy-preserving approaches for multi-centre model development where feasible, with secure aggregation and documented governance agreements. (ScienceDirect)
8. Institute independent clinical-AI ethics committees at tertiary hospitals to review high-risk deployments and hear patient petitions.
9. Fund methodologically rigorous post-market surveillance and bias monitoring with annual public reporting and corrective-action triggers.
10. Build professional capacity through CME/CPD modules on AI literacy, bias, consent, and documentation in AI-assisted care.

REFERENCES

1. Baker, N., & Goodman, K. W. (2023). Global health and big data: The WHO's artificial intelligence guidance. Journal of Medical Ethics, 49(10), 703–707. https://doi.org/10.1136/medethics-2023-109058. (PubMed Central)
2. Band, S. S., et al. (2023). Application of explainable artificial intelligence in medical image analysis. Informatics in Medicine Unlocked, 39, 101201. https://doi.org/10.1016/j.imu.2023.101201. (ScienceDirect)
3. Carey, S., et al. (2024). Fairness in AI for healthcare. Journal of Biomedical Informatics, 155, 104556. https://doi.org/10.1016/j.jbi.2024.104556. (ScienceDirect)
4. Common Cause v. Union of India, (2018) 5 SCC 1. Supreme Court of India. (privacylibrary.ccgnlud.org)
5. Council of the European Union & European Parliament. (2024). AI Act [Regulation of the European Parliament and of the Council]. See interaction with MDR and high-risk medical devices. (PubMed Central)
6. Dinakaran, D., et al. (2021). Telemedicine practice guidelines of India, 2020. Indian Journal of Psychological Medicine, 43(9), 861–863. https://doi.org/10.1177/0253717620958382. (PubMed Central)
7. European Commission. (n.d.). GDPR Article 9: Processing of special categories of personal data. EUR-Lex. (Scribd)
8. European Commission. (n.d.). GDPR Article 22: Automated individual decision-making, including profiling. EUR-Lex. (lawskills.in)
9. Food and Drug Administration. (2024). Predetermined Change Control Plan guidance for AI/ML-enabled medical devices. (U.S. Food and Drug Administration)
10. Hanna, M. G., et al. (2025). Ethical and bias considerations in AI/ML within pathology and medicine. Surgical Pathology Clinics, 18(1), 1–23. https://doi.org/10.1016/j.path.2024.10.005. (ScienceDirect)
11. India, Ministry of Health and Family Welfare. (2017). Medical Devices Rules, 2017. Central Drugs Standard Control Organization. (CDSCO)
12. Khan, M. M., et al. (2024). Towards secure and trusted AI in healthcare: A systematic review. Computer Networks, 245, 110692. https://doi.org/10.1016/j.comnet.2024.110692. (ScienceDirect)
13. Li, M., et al. (2025). Implementing federated learning in healthcare. Medical Image Analysis, 98, 103236. https://doi.org/10.1016/j.media.2025.103236. (ScienceDirect)
14. Medical Council of India / National Medical Commission. (2020). Telemedicine Practice Guidelines. (NMCN)
15. Mennella, C., et al. (2024). Ethical and regulatory challenges of AI in healthcare. npj Digital Medicine, 7, 65. https://doi.org/10.1038/s41746-024-01018-5. (PubMed Central)
16. Morley, J., et al. (2020). The ethics of AI in health care: A mapping review. Social Science & Medicine, 260, 113172. https://doi.org/10.1016/j.socscimed.2020.113172. (ScienceDirect)
17. Muhammad, D., et al. (2024). Systematic review of XAI in medical image analysis. Heliyon, 10(9), e29641. https://doi.org/10.1016/j.heliyon.2024.e29641. (ScienceDirect)
18. National Health Authority. (2020, rev. 2022). Health Data Management Policy, ABDM. Government of India. (PubMed Central)
19. Parmanand Katara v. Union of India, 1989 AIR 2039. Supreme Court of India. (globalhealthrights.org)
20. Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37. Supreme Court of India. (Indian Kanoon)
21. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. Supreme Court of India. (S3WaaS)
22. Puttaswamy v. Union of India (Aadhaar), (2018) 1 SCC 809. Supreme Court of India. (Manupatra Student)
23. Sadeghi, Z., et al. (2024). A review of explainable AI in healthcare. Computers in Industry, 158, 104005. https://doi.org/10.1016/j.compind.2024.104005. (ScienceDirect)
24. Selvi v. State of Karnataka, (2010) 7 SCC 263. Supreme Court of India. (S3WaaS)
25. Suchita Srivastava v. Chandigarh Administration, (2009) 9 SCC 1. Supreme Court of India. (Centre for Law & Policy Research)
26. Upreti, D., et al. (2024). A comprehensive survey on federated learning in healthcare. Journal of Biomedical Informatics, 154, 104501. https://doi.org/10.1016/j.jbi.2024.104501. (ScienceDirect)
27. WHO. (2021). Ethics and governance of artificial intelligence for health. World Health Organization. (World Health Organization)

28. WHO. (2025). Ethics and governance of AI for health: Guidance on large multimodal models. World Health Organization. (World Health Organization)
29. Xu, J., et al. (2021). Federated learning for healthcare informatics. Journal of Healthcare Informatics Research, 5(1), 1–19. https://doi.org/10.1007/s41666-020-00082-4. (PubMed)
30. IEEE Standards Association. (2022). IEEE 7002-2022: Standard for Data Privacy Process. https://standards.ieee.org/ieee/7002/6898/ (IEEE Standards Association)
31. IEEE Standards Association. (2020). IEEE 7010-2020: Recommended practice for assessing the impact of A/IS on human well-being. https://standards.ieee.org/ieee/7010/7718/ (IEEE Standards Association)
32. Central Drugs Standard Control Organization. (2017–2023). Medical Devices Rules and guidance updates. https://cdsco.gov.in/ (CDSCO)
33. Government of India. (2023). Digital Personal Data Protection Act (as introduced). PRS India. https://prsindia.org/ (PRS Legislative Research)
34. National Medical Commission. (2020). Telemedicine Practice Guidelines. https://www.mohfw.gov.in/pdf/Telemedicine.pdf (PubMed Central)
35. European Commission. (2024). AI Act and MDR interface in medical devices. (PubMed Central)
36. Food and Drug Administration. (2024). AI/ML in SaMD and Predetermined Change Control Plans. (U.S. Food and Drug Administration)
37. van Kolfschooten, H., et al. (2024). The EU Artificial Intelligence Act: Implications for healthcare. Health Policy, 128(9), 1100–1106. https://doi.org/10.1016/j.healthpol.2024.06.012. ScienceDirect. ScienceDirect
38. Sood, A., et al. (2025). Medical imaging privacy: A systematic scoping review. Journal of Biomedical Informatics: X. ScienceDirect. ScienceDirect
39. Pantanowitz, L., et al. (2024). Regulatory aspects of AI/ML in pathology. Modern Pathology. ScienceDirect. Modern Pathology
40. IEEE Standards Association. (2021). IEEE 7001-2021: Transparency of Autonomous Systems. IEEE. IEEE Standards Association
41. ISO/IEC. (2021). IEC 81001-5-1: Health software and health IT systems — Security — Activities in the product life-cycle. ISO. ISO