IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cross-Border Jurisdictional Challenges In Ai-Based Healthcare: A Comparative Legal Analysis Of India, Eu, And Us Models

[1]Nisha Harini G, [2]Shiva Janani S

[1]3rd year B.COM.,LLB(HONS), [2]3rd year B.COM.,LLB(HONS)

[1]School Of Law

[1]SASTRA Deemed University, Thanjavur, India

Abstract - Artificial intelligence (AI) is transforming healthcare via diagnosis algorithms, clinical decision support, medical imaging analysis, predictive analytics, and autonomous monitoring systems. Most of these systems are based on cross-national datasets, models, validation efforts, and cloud-based infrastructure. This cross-national feature raises significant legal and regulatory issues in data protection, liability, device certification, and ethical governance. This article presents a comparative legal-policy analysis of cross-border jurisdictional challenges in AI-based healthcare, with special reference to India's emerging regulatory stance in relation to established global models, specifically, the European Union (EU) and the United States (US). The examination combines official tools, regulatory documents, and scholarly work to determine friction areas: cross-border data flows and adequacy, AI medical system classification and pre-/post-market regulation, accountability and civil liability for algorithmic damage, and ethical guardrails in the form of fairness, bias reduction, and transparency. From India's policy papers and moral guidance, EU AI Act provisions and GDPR implications, and FDA guidance for AI/ML in medical devices, the paper provides realistic policy suggestions: interoperable regulatory frameworks, model contractual clauses for data trusts, harmonized liability rules, capacity building for regulators, and international sandboxing for joint validation and conformity assessment. The report ends on an implementable roadmap balancing patient safety and privacy with innovation and international collaboration.

Keywords - AI in healthcare, cross-border data flows, jurisdiction, India, EU AI Act, FDA SaMD, data protection, liability, medical devices.

1. Introduction

AI-based healthcare systems from image-based diagnostics through predictive risk stratification tools to clinical decision support often depend on data, model development, and cloud infrastructure that cross country borders. These transboundary flows create regulatory and governance heterogeneity since unique rules are imposed by different jurisdictions on the protection of personal data, approval of medical devices, risk classification by algorithms, and post-market surveillance. This mismatch can hinder cross-border collaboration in research, delay market entry, and leave outstanding exposure to liability when harm happens across borders. India, with its fast-evolving health sector and thriving ecosystem of AI, is openly crafting policy tools and ethical standards to regulate AI in health [1][2]; the EU and US, meanwhile, have launched or updated regulatory regimes with explicit implications for cross-border implementations [3][5]. This research compares India's path to international best practices and suggests a policy architecture to balance innovation with patient safeguarding.

2. Methods and Scope

This article follows a comparative legal-analytical approach. Primary sources are national legislation, formal policy documents, regulatory documents, and international standards. The main documents referred to are: India's NITI Aayog and sector guidance [1][13], Digital Personal Data Protection Act [11] (and commentaries), Indian Council of Medical Research (ICMR) ethical guidelines for AI in healthcare [2], the EU Artificial Intelligence Act and GDPR research [3][15], and FDA documentation on AI/ML-enabled medical devices [5][6] and SaMD. Secondary sources cover IAPP analysis of cross-border flows, [4] peer-reviewed articles on AI governance [7][14], and think-tank reports [9][10][17]. Analysis focuses on

a) Data flows and privacy
b) Classification of devices and regulatory compliance
c) Liability and responsibility
d) Ethical protection and fairness and
e) Policy instruments enabling cross-border collaboration.

3. Background: Why Cross-Border Jurisdiction is Important for AI Healthcare

3.1. The technical realities

AI clinical systems typically need big, heterogeneous datasets for training, validation, and performance tracking. Data subjects, model creators, and cloud service providers can be situated in several jurisdictions. Most commercial AI health services use a model in which training takes place in a jurisdiction with liberal data access and deployment in another with varying safety and privacy regulations. This technical-economic setup establishes legal contacts across borders, with issues of applicable law, permissible transfers, and who has the enforcing authority [4].

3.2. Friction points under law and regulation

Cross-border data transfers and various levels of data protection standards (i.e., GDPR adequacy vs contractual protections) influence dataset mobility [3][4]. Device classification and market access regulation of AI as medical devices are not uniform various jurisdictions classify AI as high-risk with strict conformity assessment requirements [3][5]. Liability and responsibility uncertainty regarding whether developers, deployers (platforms/hospitals), or cloud providers are responsible when algorithmic suggestions cause patient harm [7][14]. Ethical and fairness concerns, algorithmic prejudice, representativeness of populations in datasets, and disparate access to AI health tools raise cross-border ethical issues [2][10].

4. Regulatory Environments [India, EU, and US (limited comparison)]

4.1. India: changing systems and pragmatic realities

India is constructively developing a governance climate for AI and digital health that seeks to harmonize innovation with citizen safeguards. Major aspects:

All in all, India is pragmatic and innovation-friendly in its approach, but maturing when it comes to formalized, enforceable cross-border regulatory frameworks.

Ethical principles for health-AI: ICMR and other organizations have come out with ethical guidelines for healthcare-AI that emphasize human control, data minimization, and fairness [2].

Policy and strategy: The efforts of NITI Aayog and other government strategy documents have placed a focus on AI in focus areas such as healthcare; India's policy focus has been towards facilitating public and private partnerships [1][13], encouraging responsible AI, and establishing standards. (NITI Aayog)

Regime of data protection: India's Digital Personal Data Protection Act (DPDPA) and related guidance establish rules of transfer and obligations, yet commentators identify areas of uncertainty regarding health information, clinical exceptions, and real-world implementation in telehealth settings [11][18]. Current literature points to uncertainties for clinical teleconsulting and retrospective clinical data use for training AI.[14] (PMC)

Regulating medical devices: The Central Drugs Standard Control Organization (CDSCO) has started putting software and AI into use in medical device regulation, but India has no completely mature, AI-centric regulatory framework like the EU or US prewritten plans. Institutional capacity for implementation and expertise are problems [12].

4.2. European Union: risk-based, prescriptive regulation

The EU implemented the Artificial Intelligence Act [3][15] to set up a risk-based approach treating medical AI systems as "high-risk" with conformity assessments, transparency requirements, technical documentation, and post-market surveillance. Major characteristics:

High-risk designation: AI in medical devices or clinical decision-making is generally in high-risk categories, triggering stringent pre-market and post-market requirements.

GDPR implications: Rules of data protection and cross-border transfer of personal data (GDPR) place further restrictions, such as adequacy decisions or transfer mechanisms for the use of EU personal data outside the Union.

Conformity timeline & enforcement: Notified bodies and member states perform conformity assessment mechanisms; timelines for transition may be long for advanced health-AI products.

The EU approach is rights-oriented and prescriptive, but it raises compliance costs and de facto trade frictions for developers outside the EU.

4.3. United States: sectoral, flexible regulation with a focus on safety

The US regulatory environment is sectoral: medical devices (including SaMD) are regulated by the Food and Drug Administration (FDA), and privacy is subject to a patchwork of sectoral legislation [5][6] (e.g., HIPAA) and state privacy law [4]. Characteristics include:

FDA SaMD & AI/ML guidance: The FDA has released successive guidance on "good machine learning practice," predetermined change control plans (PCCPs), and transparency for machine learning-enabled devices. The agency stresses adaptive regulatory pathways that allow post-market learning while obtaining assurances of safety and effectiveness. (U.S. Food and Drug Administration)

Framework of privacy: The US is more dependent upon sectoral protection (HIPAA for covered entities) and contractual/technological safeguards for cross-border data transfers than on omnibus federal data protection like that of GDPR. (IAPP)

The US model prioritizes flexibility and quick access to the market, but creates gaps in harmonized consumer protection of data relative to the EU.

5. Cross-Border Data Flows: Legal Mechanisms and Practical Barriers

5.1. Transfer mechanisms and adequacy

Cross-border health data transfers that are used to train and validate AI usually depend on one of Adequacy decisions (e.g., EU determines that a country's legislation ensures proper protection), Standard contractual clauses/model clauses, Binding corporate rules or customized contractual models, or Specific derogations/consents (narrow and usually not practical for large sets)[4][3]. (IAPP). For India–EU transfers, the lack of EU adequacy for India means developers will have to fall back on SCCs or other strong mechanisms [11]. India's DPDPA envisions cross-border transfer regulations, but operational and legal uncertainty persists regarding "trusted" jurisdictions and standards. (NITI Aayog)

5.2. Operational friction: de-identification, re-identification risk, and medical data

Health datasets are particularly vulnerable. De-identification methods do not necessarily remove re-identification risk, particularly in the presence of auxiliary datasets. This makes transfer justifications and compliance more difficult, especially under GDPR [4], where pseudonymized data is still personal data in most situations. For AI healthcare, provenance, label quality, and metadata matter restricting the efficacy of heavy anonymization without sacrificing clinical utility. (IAPP)

5.3. Technical-legal remedies proposed

Neutral third-party validators and data trusts: Legal organizations that store datasets under fiduciary obligations and provide controlled access to accredited researchers a means to balance privacy with cross-border research. Technical annexes outlining governance, purpose limitation, and auditing rights with

standardized data use agreements (DUAs). Joint validation laboratories and cross-border sandboxes for AI medical devices where regulators across jurisdictions co-validate safety and performance [4][9]. (IAPP)

6. Liability, Accountability, and Redress

6.1. Present fragmentation

Liability regimes vary significantly:

EU: The AI Liability Directive (and product liability regulations) heads toward more definite presumptions of causality for AI harms and imposes requirements on providers, with technical documentation required to allow claimants to prove causation. (ScienceDirect) [7][15]

India: Courts deal with consumer protection, tort, and medical negligence laws; there is no legislated AI liability law. This leads to case-by-case judgments with legal ambiguity for developers and healthcare providers [14].

US: Liability tends to be contingent on product liability principles and clinical malpractice law; courts are in the process of establishing standards for harms brought about by algorithms [3][7].

Cross-border cases e.g., an EU patient injured by an algorithm created and hosted in India create choice-of-law and enforcement questions: whose standards apply, and how are judgments enforced? The absence of harmonized tort or product liability rules for AI raises risk and may discourage cross-border deployment. (Artificial Intelligence Act)

6.2. Policy recommendations to mitigate legal uncertainty

Standardized minimum requirements of safety and documentation (technical specification, origin) to establish interoperability between liability regimes. Interoperability through mandatory transparency and logging (audit trails) to support causal attribution in litigations. Insurance and risk-sharing frameworks to assign exposure to developers, cloud hosts, and deployers. Choice-of-law clauses and forum selection in contracts although beneficial need to be supplemented with substantive protections, since consumer protection regulation can prevail over forum clauses in certain jurisdictions [3][7]. (Artificial Intelligence Act)

7. Pre- and Post-Market Regulation of AI Medical Systems

7.1. Classification and conformity

The EU AI Act puts stress on the classification of high-risk systems and demands conformity assessments for medical AI. The US FDA focuses on safety and efficacy, endorsing pre-approved change control plans to support models that learn post-deployment. India is bringing AI into its world of medical device regulations, but it does not have a fully developed AI-specific conformity framework at scale. These differing strategies pose practical and regulatory hurdles for products pursuing multiple approvals in the marketplace [3][5][6][12].

7.2. Post-market surveillance and model drift

One specific challenge to adaptive AI models is model drift over time, performance alters as data distributions change. Effective post-market surveillance is required (ongoing monitoring, regular revalidation, and reporting requirements). Regulatory frameworks are being reformed to demand increased post-market transparency and monitoring strategies. India will require investment in technical capacity to analyse post-market data and implement corrective measures [5][12]. (U.S. Food and Drug Administration)

8. Ethical and Equity Considerations

AI medicine poses algorithmic bias and unequal access risks. Datasets lacking representation of some groups (e.g., rural groups, ethnic minorities) may result in biased estimates and less favourable health outcomes. India's ethical framework identifies these risks and emphasizes human control and fairness by design; global tools (WHO, OECD) also focus on human-led AI. A cross-border strategy must therefore encompass representativeness standards, fairness audits, and equitable benefit-sharing standards [2][9][10]. (Indian Council of Medical Research)

9. Policy Suggestions (Practical & Prioritized)

The following practical policy suggestions balance cross-border cooperation and protection objectives. Each suggestion has steps for implementation.

9.1. Implement interoperable minimum standards (short-term)

India must implement a technical minimum dataset and documentation standard for medical AI (data provenance, labelling standards, model cards) that aligns with OECD/WHO guidance and EU technical documentation requirements. This minimizes friction in conformity evaluations [3][9].

9.2. Establish controlled cross-border Data Trusts and DUA templates (short-to-mid- term)

Cured datasets can be hosted by the government or neutral parties and bound by purpose limitation, access restrictions, and auditing. Offer standard contractual clauses for secure transfers and include technical controls (secure enclaves, differential privacy) where appropriate [11][4]. Example clause in Annex A.

9.3. Harmonize disclosure and liability apportionment rules (mid-term)

India should operate through bilateral and multilateral forums to create a "model AI liability framework" that deals with causation, compulsory logging, and minimum insurance. This minimizes chilling effects on cross-border medical AI research and commerce[7].

9.4. Regulatory sandboxes & joint conformity labs (short-to-mid-term)

Create global sandboxes under which regulators from India, the EU member states, and the US (or their respective agencies) co-assess AI tools with standardized protocols. Sandboxes allow simultaneous testing on multi-jurisdictional parameters and can serve as a foundation for mutual recognition arrangements [5][6].

9.5. Institutional building and capacity strengthening (continuous)

Invest in institutional capacity (CDSCO, clinical validation labs) to conduct technical reviews, post-market monitoring, and audits. Leverage public–private partnerships for upskilling regulators and clinicians for AI literacy [1][12].

9.6. Foster transparency and public accountability (recurring)

Require model cards, clinical validation reports, and patient-facing disclosures for high-risk AI systems; mandate local language disclosures in India to facilitate informed consent and clinician oversight [5][6].

10. Comparative Case Studies (illustrative)

Case study A: Diagnostic imaging AI learned in Europe, implemented in India

Issues:

Provenance of data, performance over population variations, clinical validation evidence transfer, EU AI Act conformity assessment, and local CDSCO certification. Suggested process:

1. Documentation of demographics of training dataset
2. Revalidation of performance on local Indian cohorts
3. Contractual transfer or data trust access for EU-India transfers
4. Dual regulatory approval through joint sandbox testing [3][12]

Case study B: Remote monitoring AI located on US cloud, accessed by EU hospitals

Issues:

GDPR cross-border transfer provisions, SCCs or EU Standard Contractual Clauses, EU high-risk rules accountability, and FDA SaMD implications for the vendor. Recommended process: Leverage SCCs with strong technical controls, develop monitoring plans to identify drift, and incorporate PCCPs for permissible post-market model changes [5][6].

11. Limitations and Areas for Future Research

The research integrates legal, regulatory, and policy documents to date, but quick policy changes (new advice, judicial rulings) may shift the legal landscape. Future empirical work will measure the impact of cross-border regulations on AI healthcare startup deployment timelines and expenses and assess sandbox performances. Cross-border AI harm comparative litigation analyses would further illuminate jurisdictional enforcement realities [7][14].

12. Conclusion

AI healthcare is designed to be transnational. Lacking interoperable governance addressing cross-border data flows, device conformity, liability, and ethics, the potential of AI will be spottily realized and accompanied by unnecessary harms. India is getting set to leverage gains from AI in healthcare, but it needs to speed up working towards bringing technical documentation, mechanisms for data transfer, and regulatory capacity in line with international norms. Attaining this calls for a realistic combination of domestic institutional build-out, global collaboration (sandboxes, data trusts, model contractual clauses), and harmonized minimum standards protecting patients but facilitating sensible innovation [1][3][5].

Annex A : Model clauses and templates (select excerpts) (Illustrative)

These are brief, practical templates for incorporation in data-sharing contracts, device supply agreements, or cross-border DUAs. They are illustrative and should be customized by counsel for specific deals.

A.1 Sample Transfer and Processing Clause (short form)

"Data Provider will transfer pseudonymized patient datasets to Data Receiver for purposes of [model development/validation] only. Data Receiver will put in place technical and organisational measures comparable to [insert standard: e.g., GDPR Article 32-level measures], and shall not further transfer the data outside jurisdictions listed in Annex X without Data Provider's advance written authorisation. Data Receiver will use the data solely for the agreed purpose, keep an auditable processing log, and apply differential privacy or other de-identification as set out in Annex Y. Any breach of personal data must be notified to Data Provider and to the relevant supervisory authority immediately, and remediation actions must be taken within 72 hours of identification." (Include retention, deletion, and audit rights.) (IAPP)

A.2 Model Card / Technical Disclosure checklist (summary)

a) Model name, version, developer contact
b) Description of training data (size, demographics, source jurisdictions)
c) Use case and contraindications
d) Internal and external cohort performance metrics (sensitivity, specificity)
e) Known limitations and fairness audits (disaggregated metrics by demographic groups)
f) Update strategy and PCCP (if applicable). (U.S. Food and Drug Administration)

A.3 International sandbox MOU core elements

a) Scope of governance (range of AI medical devices covered);
b) Mutual validation protocols
c) Governance of data (who keeps training/validation datasets and under what control do they provide access)
d) Provision for provisional joint findings and possible mutual recognition
e) Provisions for dispute resolution. (U.S. Food and Drug Administration)

REFERENCES

[1] NITI Aayog. National Strategy for Artificial Intelligence – #AIforAll. Government of India, 2018 (https://www.niti.gov.in/).

[2] Indian Council of Medical Research (ICMR). Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare. ICMR, 2023(https://www.icmr.gov.in/).

[3] European Commission. Artificial Intelligence Act – Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act). 2021/0106(COD), Brussels: European Commission, 2024.

[4] IAPP (International Association of Privacy Professionals). "Cross-Border Data Flows and Privacy Risks in AI-Enabled Medical Devices: A Call for Guardrails." IAPP News Analysis, 2023(https://iapp.org/).

[5] U.S. Food and Drug Administration (FDA). Artificial Intelligence and Machine Learning in Software as a Medical Device (SaMD). FDA Guidance Documents, 2023–2025(https://www.fda.gov/medical-devices).

[6] FDA. Predetermined Change Control Plans for Medical Devices: Guidance for Industry and FDA Staff. U.S. FDA, 2023(https://www.fda.gov/regulatory-information/search-fda-guidance-documents/predetermined-change-control-plans-medical-devices).

[7] ScienceDirect. "AI Liability Directive and Product Liability Modernization in the EU." Computer Law & Security Review, Elsevier, 2023.

[8] Privacy Commissioner of Canada (IAPP Resource). "Health Privacy and International Data Transfer Guidance." IAPP Resource Centre, 2024.

[9] OECD. Recommendation of the Council on Artificial Intelligence. Organisation for Economic Co-operation and Development,2019.

[10] World Health Organization. Ethics and Governance of Artificial Intelligence for Health: WHO Guidance. Geneva: WHO, 2021.

[11] Digital Personal Data Protection Act, 2023 (DPDPA). Government of India. Gazette of India, August 2023.

[12] Central Drugs Standard Control Organization (CDSCO). Guidance on Software and AI-based Medical Devices. Ministry of Health & Family Welfare, India, 2024.

[13] NITI Aayog. Responsible AI for All – Approach Paper. Government of India, 2021.

[14] PMC (PubMed Central). "Legal and Ethical Challenges of AI in Healthcare: A Global Review." Frontiers in Digital Health, 2023.

[15] European Data Protection Board (EDPB). Guidelines 05/2021 on the Interplay between the GDPR and AI Act Provisions, Brussels, 2023.

[16] United Nations Educational, Scientific and Cultural Organization (UNESCO). Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021.

[17] WHO & OECD Joint Report. AI in Health: Policy and Governance Challenges, 2022.

[18] Indian Ministry of Electronics and IT (MeitY). National Data Governance Framework Policy, 2023.

[19] NIST (National Institute of Standards and Technology). AI Risk Management Framework (AI RMF 1.0), U.S. Department of Commerce, 2023.

[20] Health Canada. Regulatory Considerations for Machine Learning–Enabled Medical Devices, Ottawa, 2024.