Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 3

ISSN: 1540-3270

Legal and Regulatory Challenges of Artificial Intelligence in Healthcare Startups: A Narrative Review

Dr. Baijnath Das[1], Shivam Agarwal[1*],

College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.

Corresponding author: Shivam Agarwal,

College of Allied and Healthcare Sciences, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India.

Abstract:

Artificial intelligence (AI) startups are developing tools for diagnosis, triage, clinical decision support, remote monitoring and health-system administration. Their translation is governed by overlapping requirements for medical devices, data protection, biomedical research, professional practice, cybersecurity, consumer protection and intellectual property. This narrative review examines the principal legal and regulatory challenges faced by healthcare AI startups, with India as the primary jurisdiction and the European Union and United States as comparators. Openly accessible peer-reviewed literature and official regulatory materials published from January 2018 to August 2026 were reviewed, together with earlier foundational instruments. The analysis identifies six recurrent pressure points: uncertain product classification; evidence requirements that may not fit rapidly changing software; lawful access to representative health data; bias, transparency and human oversight; fragmented liability across developers, clinicians and institutions; and inconsistent rules across export markets. India now has a more defined policy environment through the Medical Devices Rules, the 2026 guidance on medical device software, the Digital Personal Data Protection framework, the Indian Council of Medical Research ethical guidelines and national AI-governance guidance. These instruments are complementary, but their scopes, commencement schedules and enforcement routes are not identical. Startups should therefore treat compliance as a product-lifecycle function: define intended use before development, establish data provenance and contractual rights, generate population-relevant clinical evidence, document human oversight, control software changes, allocate responsibility contractually and monitor performance after deployment. Proportionate regulatory support, common technical standards, regulatory sandboxes and clearer coordination among health, data and AI authorities could reduce uncertainty without lowering patient-safety safeguards.

Keywords: data governance; digital health; medical device software; patient safety; product liability

Introduction

Artificial intelligence (AI) is moving from research demonstrations into clinical decision support, medical imaging, triage, monitoring and administrative workflows. Translation remains difficult because technical accuracy alone does not establish clinical benefit, safety or fit with a healthcare system. Poorly defined intended use, non-representative data, weak external validation and inadequate workflow design can prevent a promising model from producing reliable clinical value.[1] The World Health Organization (WHO) has consequently framed health AI as a lifecycle governance problem requiring protection of autonomy, safety, transparency, accountability, equity and sustainability.[2]

Healthcare startups face a distinctive version of this problem. They often develop a minimum viable product while the medical purpose, user population, business model and deployment setting are still changing. Each change may alter device classification, evidence requirements, privacy roles, liability allocation or the claims that may lawfully be made. The legal environment is also layered: data law may apply before a product is a medical device, research ethics may apply before commercial launch, and professional or consumer law may apply during use. Published analyses consistently describe privacy, liability, regulatory approval, intellectual property and cross-border compliance as interdependent rather than isolated issues.[3,4]

This narrative review examines those challenges with India as the principal jurisdiction and selected comparisons with the European Union (EU) and United States (US). It focuses on practical implications for startups developing software that informs or supports healthcare decisions and on regulatory strategies that preserve innovation without weakening patient protection.

Methods

The review was structured with reference to the Scale for the Assessment of Narrative Review Articles.[5] PubMed/MEDLINE was searched for English-language material published from 1 January 2018 to 24 August 2026. Targeted web searches identified supplementary peer-reviewed material and official regulatory documents. Earlier documents were retained when they constituted a foundational law, standard or guidance. Search concepts combined "artificial intelligence", "machine learning", "healthcare", "startup", "software as a medical device", "medical device software", "regulation", "law", "liability", "data protection", "privacy", "bias", "cybersecurity", "intellectual property", "India", "European Union" and "United States".

Official sources were searched separately, including the Indian Council of Medical Research (ICMR), Central Drugs Standard Control Organisation (CDSCO), Ministry of Electronics and Information Technology, National Health Authority, Indian Patent Office, WHO, European Commission and US Food and Drug Administration (FDA). Peer-reviewed papers were included when they addressed regulation, governance, evidence, liability or implementation of clinical AI. Statutes, rules and regulator guidance were prioritised for statements of law. Only sources with openly accessible full text were retained. Selection was purposive and thematic; no pooled effect estimates or formal risk-of-bias assessment was undertaken. Regulatory status was checked to 24 August 2026.

The regulatory perimeter in India

India does not presently regulate every healthcare AI application through one AI-specific statute. Instead, applicable duties depend on the product's intended purpose, risk, data practices and place in the clinical pathway. The ICMR's 2023 ethical guidelines address AI across biomedical research and healthcare and emphasise autonomy, safety, accountability, transparency, fairness, data privacy and stakeholder responsibility.[6] The India AI Governance Guidelines, issued in 2025, add a cross-sector, principle-based framework centred on trust, people-first design, fairness, accountability, understandability, safety and resilience.[7] These instruments are influential governance benchmarks, but they do not replace binding sectoral law.

Where software meets the statutory definition of a medical device, the Drugs and Cosmetics Act framework and Medical Devices Rules, 2017 apply through a risk-based classification and licensing system.[8] CDSCO's final Guidance Document on Medical Device Software under the Medical Devices Rules, published on 21 July 2026, is particularly important for startups because it clarifies the treatment of standalone software and software embedded in a device, regulatory pathways, documentation, clinical evidence, quality management, change control and post-market responsibilities.[9] Classification turns on intended medical purpose rather than the developer's description of the product as an "AI platform", "wellness tool" or "decision aid". Apps that remain outside device regulation may still be governed by data protection, telemedicine, advertising, professional-practice and consumer-protection rules; analyses of mental-health apps in India illustrate how these regimes can overlap even when device status is uncertain.[10]

For a startup, the practical lesson is to freeze an intended-use statement before model validation. The statement should identify the clinical task, target population, user, input, output, care setting and consequence of an erroneous result. A later pivot from workflow support to diagnosis, or from clinician-facing to patient-facing use, may require reclassification, new evidence, revised labelling and different controls.

Data protection, consent and cybersecurity

Health AI depends on longitudinal, diverse and frequently identifiable data. Under India's Digital Personal Data Protection Act, 2023, a startup that determines the purpose and means of processing digital personal data may be a Data Fiduciary and remains responsible for processing performed through a Data Processor. Where consent is relied upon, it must be free, specific, informed, unconditional and unambiguous; the Act also permits processing

for specified "certain legitimate uses" and provides rights concerning access, correction, erasure and grievance redressal.[11] The Digital Personal Data Protection Rules, 2025 introduce more detailed notice, security, breach, consent-manager and other operational requirements through staggered commencement.[12] Consequently, a startup should not assume that every provision became operative on the same date.

Clinical consent, research consent and data-protection consent are related but not interchangeable. A hospital's authority to treat a patient does not automatically grant a startup unlimited right to train, commercialise or transfer a model. Contracts must identify the parties' data roles; authorised purposes; provenance and quality of data; de-identification or pseudonymisation method; retention; subcontractors; security controls; audit rights; breach response; model-derived artefacts; and deletion or return at termination. Indian-focused reviews also identify continuing challenges around secondary use, privacy, security and institutional capacity.[13]

De-identification reduces risk but does not guarantee anonymity, particularly for genomic, imaging and longitudinal records. Data minimisation, purpose limitation, role-based access, encryption, logging, separation of identifiers, secure development and documented threat modelling should therefore be incorporated by design. Cybersecurity is simultaneously a privacy, safety and continuity issue: corrupted inputs, model theft or unavailable services can affect care. India's Computer Emergency Response Team directions impose incident-reporting and log-related duties on covered entities, while device-specific security obligations may also apply.[14] Cross-border cloud services require a documented transfer analysis rather than an unsupported assumption that Indian law either prohibits or freely permits every transfer.

Evidence, bias and lifecycle control

Regulatory clearance is not established by a high area under the curve on a retrospective development dataset. Evidence should match the claim and include analytical validation, clinical validation and, where relevant, clinical utility, human-factors assessment and comparison with current care. Local performance can vary with prevalence, equipment, workflow, language and demographic composition. A scoping review of 692 FDA-authorised AI or machine-learning devices found that race or ethnicity was reported for only 3.6 per cent, age was unreported in 81.6 per cent, and prospective post-market surveillance was described for 9.0 per cent, demonstrating persistent transparency gaps.[15]

Bias is therefore both a patient-safety risk and a legal risk. Startups should pre-specify subgroup analyses, clinically meaningful endpoints, failure thresholds and escalation pathways; report missingness and dataset shift; and validate at sites not used for training. The FUTURE-AI consensus framework translates fairness, universality, traceability, usability, robustness and explainability into lifecycle practices.[16] For clinical studies, CONSORT-AI, SPIRIT-AI and DECIDE-AI provide complementary reporting standards for trials, protocols and early live evaluation.[17-19] These standards do not confer regulatory approval, but they improve the completeness and auditability of evidence.

Model updates create a second challenge. A locked model can degrade as disease prevalence, scanners, coding or clinical practice changes; an adaptive model may change the regulated product after approval. WHO recommends total-product-lifecycle oversight, clear intended use, external validation, transparency, human intervention, cybersecurity and post-market monitoring.[20] Post-market plans should define drift metrics, subgroup surveillance, incident triage, rollback, version control and triggers for regulatory notification or renewed validation. European radiology experts similarly recommend continuous performance, safety and bias monitoring with clear responsibilities across manufacturers and deploying institutions.[21]

Accountability, professional duties and liability

When an AI-supported decision causes harm, responsibility may be distributed among the developer, data supplier, cloud vendor, hospital and clinician. The relevant questions include whether the system was defective; whether evidence and warnings were adequate; whether deployment departed from the intended use; whether a clinician reasonably relied on or overrode the output; and whether monitoring detected a known failure. Reviews of diagnostic AI liability find no universally accepted rule that assigns responsibility to a single actor.[22]

In India, potential claims may arise through negligence, contract, consumer protection, product liability and sectoral medical-device obligations. The Consumer Protection Act, 2019 contains product-liability provisions applicable to manufacturers, service providers and sellers in defined circumstances.[23] A disclaimer that an output is "for information only" will not necessarily control the legal analysis if the product is designed, marketed and used for a medical purpose. Startups should specify who may use the system, the degree of human review, known limitations, contraindicated settings, training needs, incident reporting and response times. Contracts should allocate operational duties and indemnities, but contractual allocation cannot remove statutory duties or the clinician's independent professional obligations.

Intellectual property and commercial contracting

A healthcare AI product commonly combines source code, model weights, curated data, annotations, documentation, trade secrets, trademarks and inventions. Ownership should be resolved before development involving founders, employees, contractors, hospitals or universities. The 2026 WHO-International Telecommunication Union-World Intellectual Property Organization guide stresses that intellectual property, commercialisation, health-data governance and standards must be planned together across the innovation lifecycle.[24]

In India, patentability of computer-related inventions is assessed under section 3(k) of the Patents Act and the current Computer Related Inventions Guidelines; a software label alone neither secures nor necessarily defeats patentability, and the claimed technical contribution is material.[25] Copyright may protect code and certain original expression, but it does not by itself grant permission to use third-party clinical data, annotations or copyrighted material for training.[26] Startups should perform freedom-to-operate and data-rights reviews, secure written assignments and licences, protect trade secrets, record open-source obligations, and address ownership of improvements, feedback and model outputs in hospital and vendor contracts.

Cross-border market access

A product that can be distributed globally is not regulated globally through one approval. In the EU, medical-purpose AI may be governed concurrently by the Medical Device Regulation or In Vitro Diagnostic Medical Device Regulation, the General Data Protection Regulation and the AI Act.[27-29] The AI Act entered into force in 2024; following the 2026 AI Omnibus changes, rules for specified high-risk systems and AI embedded in regulated products follow extended transition dates. Startups should therefore verify the date and category applicable to their own product rather than rely on the general commencement date.

In the US, the FDA regulates AI-enabled device software through established device pathways. Its 2025 draft lifecycle and marketing-submission guidance describes documentation for data management, model description, performance, human factors, transparency, cybersecurity and monitoring.[30] Final 2025 guidance on predetermined change control plans permits a developer to propose bounded future modifications and a method for implementing and assessing them.[31] Comparative research has shown substantial differences in approval routes and public transparency between the US and Europe, while later mapping studies describe continuing overlap among AI, device and data regimes.[32,33] International harmonisation efforts can reduce duplication, but they do not create automatic mutual recognition.[34] Table I summarises selected differences relevant to startup planning.

Table I. Selected jurisdictional requirements relevant to healthcare artificial-intelligence startups

Domain	India	European Union	United States	Startup implication
AI-specific layer	2025 India AI Governance Guidelines are principle-based; sectoral laws remain decisive.	AI Act uses risk tiers; high-risk dates were extended by the 2026 AI Omnibus.	No single cross-sector federal AI Act for health products.	Map every claim to binding sectoral rules; do not treat an ethics framework as market authorisation.

Medical-device route	Medical Devices Rules, 2017; CDSCO medical-device-software guidance (2026).	MDR/IVDR conformity assessment, with AI Act interaction where applicable.	FDA 510(k), De Novo or premarket approval pathway according to device status and risk.	Fix intended use and classification early; budget evidence and quality-system work before launch.
Personal data	DPDP Act, 2023 and Rules, 2025 with staged commencement; other sectoral duties may apply.	GDPR protects health data as a special category and requires a lawful basis and Article 9 condition.	HIPAA applies to covered entities/business associates; other federal and State rules may cover products outside HIPAA.	Determine data roles and lawful bases per deployment; contract for processor, cloud and hospital responsibilities.
Model change	2026 CDSCO guidance addresses change control and regulatory consequences for medical-device software.	Substantial modification may trigger renewed conformity assessment.	FDA predetermined change control plans can prospectively describe bounded modifications.	Maintain version control, pre-specified change boundaries, validation and regulatory impact assessment.
Post-market phase	Medical-device vigilance, complaint handling and software monitoring depend on product class and licence.	MDR/IVDR vigilance plus AI Act monitoring where applicable.	Medical-device reporting, corrections/recalls and lifecycle monitoring apply as relevant.	Contract for access to real-world performance data, subgroup monitoring, incident investigation and rollback.

Note: Regulatory status is summarised as of 24 August 2026; product-specific requirements depend on intended use, risk and deployment context. Sources: refs. [8,9,11,12,27-31,40]

A lifecycle compliance model for startups

Compliance should be treated as an engineering workstream rather than a final pre-launch review. Interviews with medical-AI developers show that regulatory knowledge, data governance and risk management influence development choices, particularly for higher-risk products.[35] A proportionate startup model can be organised around seven decision gates (Table II).

Table II. Lifecycle compliance gates for a healthcare artificial-intelligence startup

Lifecycle gate	Minimum controlled record	Principal failure avoided	Release decision
1. Intended use	Clinical task, user, population, input, output, setting and consequence of error	Borderline or incorrect classification; unsupported claims	No development claim proceeds without clinical and regulatory sign-off
2. Data access	Provenance, permission, data roles, consent or other basis, retention and security	Unlawful processing; leakage; unusable training data	No ingestion until rights, purpose and safeguards are documented

3. Model development	Versioned code, dataset lineage, design controls, threat model and risk register	Irreproducibility; hidden change; unmanaged cybersecurity risk	No candidate model without traceable build and risk review
4. Validation	Pre-specified protocol, external sites, subgroup results, human factors and acceptance limits	Performance inflation; bias; unsafe workflow interaction	No clinical claim unless evidence matches the intended use
5. Market access	Classification rationale, quality documents, technical file, labelling and regulator correspondence	Launch without required authorisation or misleading promotion	No commercial release before jurisdictional requirements are met
6. Deployment	Integration plan, user training, oversight, responsibilities, service levels and incident procedure	Automation bias; responsibility gaps; delayed response	No site go-live without accountable owners and safe fallback
7. Monitoring and change	Drift and subgroup metrics, complaints, corrective action, rollback and change assessment	Silent degradation; uncontrolled adaptive updates	No update until validation and regulatory impact are approved

Note: Each gate should be proportionate to product risk and documented within the quality-management system.

First, governance should be assigned to named individuals with authority over clinical safety, data protection, quality and cybersecurity. The same person may cover more than one role in a small company, but responsibilities and escalation must be documented. Secondly, a regulatory inventory should map each product claim and deployment country to device, research, data, professional, advertising, consumer and cybersecurity requirements. Thirdly, a living evidence plan should connect every claim to a dataset, protocol, acceptance criterion and report.

Fourthly, technical documentation should preserve the lineage of data, code, model versions, validation, known limitations and changes. Fifthly, contracts should reflect the actual operational chain, including hospital integration, cloud hosting, clinical oversight, user training, incident investigation and post-market data access. Sixthly, release management should prevent unreviewed model or interface changes from bypassing validation. Finally, the board and investors should receive concise compliance indicators such as unresolved safety risks, subgroup performance, drift, incidents, overdue corrective actions and regulatory commitments. Organisational governance case studies indicate that multidisciplinary review and monitoring can be implemented without eliminating local innovation.[36]

Generative and general-purpose models require additional caution because outputs may be non-deterministic, difficult to trace and capable of producing persuasive false information. WHO guidance recommends clear task definition, stakeholder participation, independent assessment, transparency, cybersecurity and post-release auditing for large multimodal models used in health.[37] A startup that incorporates a third-party foundation model must still validate the complete system, control updates, document vendor dependencies and maintain a safe fallback.

Policy priorities and limitations

India's 2026 medical-device-software guidance materially improves product-specific clarity. Further progress could come from coordinated interpretations across CDSCO, ICMR, data-protection and AI-governance bodies; regulator-issued examples for borderline clinical software; common expectations for representative datasets and

algorithm-change protocols; public summaries of evidence and adverse events; and supervised sandboxes linked to defined exit criteria. Global reviews similarly support lifecycle-based, risk-proportionate regulation and stronger clinical-trial and post-market expectations.[38,39] Support for startups should reduce duplicated procedure, not reduce the evidence required for higher-risk clinical claims.

This review is limited by its narrative design, English-language restriction and selective jurisdictional comparison. Rapid policy change may make individual procedural details time-sensitive. It does not provide a legal opinion on a specific product, and jurisdiction-specific advice remains necessary. Its strength is the integration of openly accessible legal, regulatory and biomedical sources into a startup-focused lifecycle framework.

Conclusion

The central regulatory challenge for healthcare AI startups is not the absence of every rule, but the interaction of rules that attach to different stages, actors and risks. In India, recent data-protection rules, AI-governance guidance and medical-device-software guidance provide a clearer foundation, while ICMR ethical standards remain important for research and clinical use. A defensible startup pathway begins with precise intended use and continues through lawful data access, representative evidence, transparent human oversight, controlled updates, cybersecurity, contractual accountability and post-market monitoring. Early integration of these functions can reduce regulatory rework and improve patient safety. Regulators can complement this approach through coordinated guidance, proportional oversight, interoperable standards and transparent pathways for clinically responsible innovation.

Declaration

- Acknowledgment: None.
- Financial support & sponsorship: None.
- Conflicts of Interest: None.
- Ethical approval: Not applicable.
- Data availability: No new research data were generated or analysed. All sources used in the review are cited and were openly accessible at the time of the search.

References:

[1] Kelly CJ, Karthikesalingam A, Suleyman M, Corrado G, King D. Key challenges for delivering clinical impact with artificial intelligence. BMC Med. 2019;17:195. doi: 10.1186/s12916-019-1426-2.

[2] World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO; 2021. Available from: https://www.who.int/publications/i/item/9789240029200, accessed on August 24, 2026.

[3] Pham T. Ethical and legal considerations in healthcare AI: Innovation and policy for safe and fair use. R Soc Open Sci. 2025;12:241873. doi: 10.1098/rsos.241873.

[4] Palaniappan K, Lin EYT, Vogel S. Global regulatory frameworks for the use of artificial intelligence (AI) in the healthcare services sector. Healthcare (Basel). 2024;12:562. doi: 10.3390/healthcare12050562.

[5] Baethge C, Goldbeck-Wood S, Mertens S. SANRA-a scale for the quality assessment of narrative review articles. Res Integr Peer Rev. 2019;4:5. doi: 10.1186/s41073-019-0064-8.

[6] Indian Council of Medical Research. Ethical guidelines for application of artificial intelligence in biomedical research and healthcare. New Delhi: ICMR; 2023. Available from: https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare, accessed on August 24, 2026.

[7] Ministry of Electronics and Information Technology. India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation. New Delhi: Government of India; 2025. Available from: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf, accessed on August 24, 2026.

[8] Central Drugs Standard Control Organisation. Medical Devices Rules, 2017, as amended. New Delhi: Directorate General of Health Services, Ministry of Health and Family Welfare. Available from:

https://cdsco.gov.in/opencms/opencms/en/Acts-and-rules/Medical-Devices-Rules/, accessed on August 24, 2026.

[9] Central Drugs Standard Control Organisation. Guidance document on Medical Device Software under MDR-2017. New Delhi: Directorate General of Health Services, Ministry of Health and Family Welfare; 2026. Available from: https://cdsco.gov.in/opencms/opencms/en/Medical-Device-Diagnostics/, accessed on August 24, 2026.

[10] Singh Sethi MI, Kumar RC, Manjunatha N, Naveen Kumar C, Math SB. Mental health apps in India: Regulatory landscape and future directions. BJPsych Int. 2025;22:2-5. doi: 10.1192/bji.2024.20.

[11] Ministry of Law and Justice. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). New Delhi: Government of India; 2023. Available from: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf, accessed on August 24, 2026.

[12] Ministry of Electronics and Information Technology. Digital Personal Data Protection Rules, 2025. Gazette of India, G.S.R. 846(E), November 13, 2025. Available from: https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf, accessed on August 24, 2026.

[13] Joshi U, Baisil S, Kini BS, Mehta M, Datta S. AI ethics in Indian healthcare: A scoping review of national and international guidelines on privacy, data protection, and security. BMC Med Ethics. 2026;27:86. doi: 10.1186/s12910-026-01435-1.

[14] Indian Computer Emergency Response Team. Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet. New Delhi: CERT-In; 2022. Available from: https://www.cert-in.org.in/Directions70B.jsp, accessed on August 24, 2026.

[15] Muralidharan V, Adewale BA, Huang CJ, Nta MT, Ademiju PO, Pathmarajah P, et al. A scoping review of reporting gaps in FDA-approved AI medical devices. NPJ Digit Med. 2024;7:273. doi: 10.1038/s41746-024-01270-x.

[16] Lekadir K, Frangi AF, Porras AR, Glocker B, Cintas C, Langlotz CP, et al. FUTURE-AI: International consensus guideline for trustworthy and deployable artificial intelligence in healthcare. BMJ. 2025;388:e081554. doi: 10.1136/bmj-2024-081554.

[17] Liu X, Cruz Rivera S, Moher D, Calvert MJ, Denniston AK; SPIRIT-AI and CONSORT-AI Working Group. Reporting guidelines for clinical trial reports for interventions involving artificial intelligence: The CONSORT-AI extension. Nat Med. 2020;26:1364-74. doi: 10.1038/s41591-020-1034-x.

[18] Cruz Rivera S, Liu X, Chan AW, Denniston AK, Calvert MJ, et al. Guidelines for clinical trial protocols for interventions involving artificial intelligence: The SPIRIT-AI extension. Nat Med. 2020;26:1351-63. doi: 10.1038/s41591-020-1037-7.

[19] Vasey B, Nagendran M, Campbell B, Clifton DA, Collins GS, Denaxas S, et al. Reporting guideline for the early stage clinical evaluation of decision support systems driven by artificial intelligence: DECIDE-AI. BMJ. 2022;377:e070904. doi: 10.1136/bmj-2022-070904.

[20] World Health Organization. Regulatory considerations on artificial intelligence for health. Geneva: WHO; 2023. Available from: https://www.who.int/publications/b/64825, accessed on August 24, 2026.

[21] Cuocolo R, Bernardini D, Pinto Dos Santos D, Klontzas ME, Akinci D'Antonoli T, Semedo LC, et al. AI medical device post-market surveillance regulations: Consensus recommendations by the European Society of Radiology. Insights Imaging. 2025;16:275. doi: 10.1186/s13244-025-02146-8.

[22] Cestonaro C, Delicati A, Marcante B, Caenazzo L, Tozzo P. Defining medical liability when artificial intelligence is applied on diagnostic algorithms: A systematic review. Front Med (Lausanne). 2023;10:1305756. doi: 10.3389/fmed.2023.1305756.

[23] Ministry of Law and Justice. The Consumer Protection Act, 2019 (No. 35 of 2019). New Delhi: Government of India; 2019. Available from: https://upload.indiacode.nic.in/showfile?actid=AC_UK_89_1171_00002_00002_1630393876767&filename=a2019-35.pdf&type=actfile, accessed on August 24, 2026.

[24] World Intellectual Property Organization, World Health Organization, International Telecommunication Union. AI-enabled health innovation and intellectual property: From idea to impact. Geneva: WIPO; 2026. Available from: https://www.wipo.int/web-publications/ai-enabled-health-innovation-and-ip-from-idea-to-impact/en/introduction.html, accessed on August 24, 2026.

[25] Office of the Controller General of Patents, Designs and Trade Marks. Guidelines for Examination of Computer Related Inventions (CRIs)-2025. New Delhi: Government of India; 2025. Available from: https://ipindia.gov.in/resource/patents-resources-guidelines, accessed on August 24, 2026.

[26] Government of India. The Copyright Act, 1957, as amended. New Delhi: Copyright Office. Available from: https://copyright.gov.in/Copyright_Act_1957/index.html, accessed on August 24, 2026.

[27] European Parliament and Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, as amended; application timeline. Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, accessed on August 24, 2026.

[28] European Parliament and Council of the European Union. Regulation (EU) 2017/745 on medical devices. Off J Eur Union. 2017;L117:1-175. Available from: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng, accessed on August 24, 2026.

[29] European Parliament and Council of the European Union. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data. Off J Eur Union. 2016;L119:1-88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, accessed on August 24, 2026.

[30] US Food and Drug Administration. Artificial intelligence-enabled device software functions: Lifecycle management and marketing submission recommendations. Draft guidance for industry and Food and Drug Administration staff. Silver Spring, MD: FDA; 2025. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/artificial-intelligence-enabled-device-software-functions-lifecycle-management-and-marketing, accessed on August 24, 2026.

[31] US Food and Drug Administration. Marketing submission recommendations for a predetermined change control plan for artificial intelligence-enabled device software functions. Guidance for industry and Food and Drug Administration staff. Silver Spring, MD: FDA; 2025. Available from: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence, accessed on August 24, 2026.

[32] Muehlematter UJ, Daniore P, Vokinger KN. Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015-20): A comparative analysis. Lancet Digit Health. 2021;3:e195-203. doi: 10.1016/S2589-7500(20)30292-2.

[33] Schmidt J, Schutte NM, Buttigieg S, Novillo-Ortiz D, Sutherland E, Anderson M, et al. Mapping the regulatory landscape for artificial intelligence in health within the European Union. NPJ Digit Med. 2024;7:229. doi: 10.1038/s41746-024-01221-6.

[34] Reddy S. Global harmonization of artificial intelligence-enabled software as a medical device regulation: Addressing challenges and unifying standards. Mayo Clin Proc Digit Health. 2025;3:100191. doi: 10.1016/j.mcpdig.2024.100191.

[35] Choo CM, Malik S, Feng M, Liu N, Lwin MO, Xu H, et al. Examining developer perspectives on medical AI regulatory frameworks. NPJ Digit Med. 2026;9:542. doi: 10.1038/s41746-026-02689-0.

[36] Kim JY, Hasan A, Kueper J, Tang T, Hayes C, Fine B, et al. Establishing organizational AI governance in healthcare: A case study in Canada. NPJ Digit Med. 2025;8:522. doi: 10.1038/s41746-025-01909-3.

[37] World Health Organization. Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models. Geneva: WHO; 2024. Available from: https://www.who.int/publications/i/item/9789240084759, accessed on August 24, 2026.

[38] Shanmugam U, Rajendran MK, Natarajan J, Karri VVSR. Clinical trial design and regulatory requirements for artificial intelligence as a medical device: A PRISMA-ScR-guided scoping review of global guidance and evidence (2017-2025). J Clin Med. 2026;15:1937. doi: 10.3390/jcm15051937.

[39] Ebad SA, Alhashmi A, Amara M, Miled AB, Saqib M. Artificial intelligence-based software as a medical device (AI-SaMD): A systematic review. Healthcare (Basel). 2025;13:817. doi: 10.3390/healthcare13070817.

[40] US Department of Health and Human Services. Health information privacy: The HIPAA Privacy Rule. Washington, DC: HHS. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html, accessed on August 24, 2026.