BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA, September 2026. Vol. **23**(3), p. 1349-1366

Regulating AI in Healthcare: Data Protection, Consent, Accountability, and Transparency

Rahul Shamota and Govind Yadav*

Department of Law, Manipal University, Jaipur, India.

http://dx.doi.org/10.13005/bbra/3577

(Received: 01 June 2026; accepted: 03 September 2026)

The speed at which AI is being used in health care and the making of clinical decisions leads to legal, ethical, and regulatory dilemmas on data protection, informed consent, clinical responsibility, and the explanation of clinical decision-making. This paper focuses on health care AI and addresses biotechnology in the context of genomic, diagnostic, drug development, and clinical services and/or health data processing. Using doctrinal and comparative legal analysis of laws, cases, regulations, policies, and relevant literature published in the European Union, the United States, India, the United Kingdom, and China, this study uses the legal cut-off date of June 30, 2026. The comparison focuses on data protection, medical liability, transparency, informed consent, and institutional accountability. It differentiates primary law from non-binding law and policy. The analysis did not find such a comprehensive health care AI system in these jurisdictions, and found remaining gaps in informed consent, distributed liability, explainability, and institutional control. It proposes providing more information to the patient, oversight by humans, and greater control over response allocations, but acknowledges that the content and the nature of the legal obligations will vary in each jurisdiction.

Keywords: Algorithmic Accountability, Artificial Intelligence, Data Protection, Health Data Governance, Healthcare Law, Patient Consent.

The Emergence of Artificial Intelligence in Healthcare

The last 20 years have brought an astonishing transformation in the relationship between artificial intelligence and healthcare, medicine, and biotechnology. Initially, these relationships involved the use of AI as experimental tools. Now, an entire range of technologies serve fundamental roles in the processes of clinical diagnostics, genomics, drug discovery, and the administration of public health and hospitals. There are many machine learning algorithms in use for the analysis of radiologic images, predicting the deterioration of patients, modeling the spread of communicable diseases, and aiding the assessment of pathology specimens. Natural language processing systems help to extract information of clinical importance from unorganized electronic health records. There are AI-empowered robotic systems that now assist in surgical procedures that previously required the exclusive skill and dexterity of human surgeons. In biotechnology, AI-based algorithmic systems facilitate the prediction of the structure of proteins, the identification of potential therapeutic candidates, and the regulation of biological data at an unmanageable scale for any human analyst.[1 11] For purposes of this article, those biotechnology applications are considered

*Corresponding author E-mail: govind.yadav@jaipur.manipal.edu

This is an Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).
Published by Oriental Scientific Publishing Company © 2026

only where they intersect with clinical care, health-data processing, or medical-device regulation; the primary analytical scope is healthcare AI.

The rapid expansion of AI technologies far outpaces our existing legal and regulatory structures. Current legal frameworks that govern the practice of medicine, the practice of pharmacy, the protection of personal data, and consumer protection laws were built for a world where technology would develop with predictability. AI is a technology that develops in fundamentally different ways. In particular, AI is opaque, probabilistic, and extremely flexible. These frameworks have not kept up and there is a situation in which powerful technologies can proliferate in clinical and biotech environments, where the protections for patients and healthcare professionals, and the concerns of regulators, are not fully addressed.[12 20]

A lack of regulatory protections creates a threat to patient safety and erodes public trust in healthcare systems. Concerns of this kind are not just theoretical. If an AI system chooses a harmful clinical pathway, existing laws on medical negligence may not identify the AI developer, the hospital, or the clinician in question. If an AI system used for healthcare purposes is involved in a data breach, the laws that protect data may not identify the AI developer in question. If a patient is harmed by an AI system that is involved in the clinical decision-making process the legal system may not identify the AI developer in question for the clinical decision-making system.[21 25]

Legal Issues Related to Automated Medical Decision-Making

There are many interconnected legal issues related to the use of AI in medical decision-making, the starting point being informed consent. The principle of informed consent, which is found in all the major legal systems as a principle of medical ethics and health law, requires that patients are provided enough information regarding the proposed course of action so that they are able to make a voluntary and informed decision regarding the care provided to them. There are several ways in which such systems make it difficult to achieve informed consent. AI outputs are often probabilistic in nature, as opposed to deterministic. In such a case, the clinician is provided with a risk score, likelihood ratio, or suggestion, which he or she must interpret as a diagnostic or some other conclusion. The clinician is then faced with the challenge of explaining to the patient the AI output, as well as the basis and limitations of the output, to the end that the patient is able to provide informed consent, a challenge to which the clinician is not prepared, either by training or by legal doctrine.[26 28]

Besides just seeking patient consent, the introduction of AI into the health sector brings with it new challenges in the realm of liability. Tort law and the law of medical negligence take into account the model of care in which an individual professional is answerable, with a duty of care owed to an identifiable patient whose conduct can be assessed against the relevant standard of practice. In many ways, AI systems defy this model. The statements made by an algorithm are a function of, and therefore a byproduct of, the underlying data and/or the statistics, and do not represent the professional's deliberation. The entities that develop, implement and operate the system are not the same. In the case of an incident, the contribution of the AI system, the practitioner, and the organization, will be difficult to separate.[29 31]

The additional challenge of data protection becomes relevant here. The majority of AI systems in healthcare rely on personal data, and in many instances, they rely on data of a sensitive nature (health records, genomic data, biometric data, and diagnostic images). The laws on the processing of personal data of a sensitive nature impose obligations on proportionality, purpose limitation, accuracy, and security; requirements that are hard to implement when dealing with systems of AI that process data at an extremely large scale. It remains uncertain in most of the world whether traditional legal grounds for processing (e.g., patient consent) are sufficient in the context of AI systems that analyze health data.[32 35]

Objectives and Research Questions

This article aims to achieve three goals. The first is to provide a high-level description of the primary legal risk categories due to the use of AI in healthcare and to identify how legal issues and frameworks could address those risk categories. The second goal is to analyze the regulatory approaches of five jurisdictions to current legal systems and formally proposed or released reforms,

as of the last date of the analysis. The final goal is to create a governance structure with patient rights, institutional accountability, and algorithmic openness as the main pillars.

The main research questions are: first, what makes the legal risks of healthcare AI distinct from the legal risks of other medical technologies? Second, how do the regulatory systems of the EU, the US, India, the UK, and China answer these risks? Finally, what new legal, regulatory, and institutional responses are needed to establish a system of enforceable rights and obligations for healthcare AI?

The main research materials and methods are explained in section 2. Section 3 presents the findings of the analysis, including comparative tables and governance frameworks. In section 4, the author discusses the major legal and policy issues. Finally, section 5 concludes the article and presents recommendations for legal reforms.

MATERIALS AND METHODS

Nature of the Research

This research combines doctrinal and comparative legal methods. It does not involve laboratory experiments, clinical trials, human participants, or animal subjects. The analysis focuses on legal texts, case law, regulatory documents, policy materials, and scholarship concerning artificial intelligence in healthcare, including biotechnology-related applications only where they intersect with clinical care, health-data processing, or medical-device regulation.

Research Materials

Primary sources are Acts and laws, case law, regulations, and official regulatory materials regarding AI, data protection, and medical devices in the healthcare sector in the EU, U.S., India, UK, and China. Official guidance along with policy and technical reports outline the way in which the implementing legislation is written, and the scholarship provides doctrinal and ethical context.

The article does not analyze primary empirical data and does not draw on original quantitative research. References to regulations, the positons of institutions and changes in policies are all derived from public official documents, as are the development trends. The context provided by the peer reviewed articles are used to draw the boundaries.

The legal cut off date is 30 June 2026. Materials were identified with the help of targeted searches of official legal portals and regulator websites, along with the peer reviewed literature. Search terms included "artificial intelligence" or "AI" along with "healthcare," "clinical decision support," "medical device," "health data," "informed consent," "automated decision-making," "explainability," "negligence," "product liability," "algorithmic bias," and "cybersecurity," paired with the respective country names. In the absence of other legal sources, regulations take precedence. Instruments were classified as either legally binding, non-binding, or policy/proposal instruments. Only legally binding instruments that were in effect by the cut-off date were considered as legally binding for the purposes of this article.

Comparative Methodology

The comparative analysis uses five jurisdictions to represent distinct regulatory models: the European Union's horizontal risk-based and data-protection framework; the United States' sectoral and agency-led model; India as the main focus jurisdiction with an evolving digital-health and data-protection framework; the United Kingdom's post-Brexit sectoral and guidance-led approach; and China's combination of personal-information and algorithm-governance rules.

In each jurisdiction, five concerns are assessed: data protection, medical liability, algorithmic transparency, patient consent, and institutional accountability. For each concern, the analysis separately identifies binding law, official guidance, and policy proposals so that recommendations are not presented as existing legal duties. This framework permits a systematic comparison of both substantive protections and the legal force of the instruments relied upon.

Ethical and Methodological Limitations

This analysis does not examine participants, focus on clinical trials, or even engage in lab work or animal research. Consequently, this analysis does not consider the need for ethics review board approval, nor does it consider the need for informed consent of participants, as would be the case in studies involving human participants. In the future though, if this framework is built upon

and further empirical research is conducted, ethical review board approval may be warranted and ought to be considered should human participants be included or primary research be conducted where identifiable data may be collected.

Overall, I acknowledge the limitations of the methodology in using this doctrinal approach. This research is primarily a legal comparison using only publicly available materials. Thus, it primarily reflects the law and regulation in force at the time of this research with respect to various implementations of law and the enforcement thereof. This analysis exclusively cites sources in the English language and, in the case of unregulated instruments in other languages, translations thereof, thereby creating gaps in the interpretative process. I recognize these limitations; however, the comparative doctrinal methodology in this case is sufficient to attain the degree of analysis required in this article and provides a basis for both legally sustainable and practically useful solutions.

RESULTS

Key Legal Risks in AI-Based Healthcare

Integrating AI into healthcare creates legal risks that may be more difficult to allocate and supervise than risks associated with many conventional medical technologies. Across the five jurisdictions, the analysis identifies seven recurring areas: informed-consent failures, algorithmic opacity, health-data protection, medical-liability gaps, discriminatory outcomes, cybersecurity risks, and institutional-accountability gaps. These risks

Table 1. Key Legal Risks in AI-Based Healthcare Systems

Legal Issue	Healthcare Context	Risk Created	Possible Regulatory Response
Informed Consent Failure	Diagnostic tools and clinical decision-support systems used without explicit patient authorisation	Violation of patient autonomy; breach of medical ethics; potential tort liability	Mandatory AI disclosure requirements; layered consent protocols; regulatory guidance
Algorithmic Opacity	Black-box deep-learning models in radiology, pathology, and genomic screening	Inability to explain clinical decisions; erosion of patient trust; judicial evidentiary challenges	Statutory explainability mandates; audit trail requirements; third-party algorithm review
Data Protection Breach	Processing of sensitive health records and biometric data by AI platforms	Unauthorised disclosure; re-identification risk; breach of constitutional privacy rights	Data minimisation obligations; privacy impact assessments; sector-specific health data laws
Medical Liability Gaps	AI-assisted diagnosis or surgical robotics where human oversight is reduced	Uncertainty over negligence attribution between developer, hospital, and clinician	Shared-liability frameworks; product liability extension to AI; mandatory insurance
Discriminatory Outcomes	Training datasets that under-represent marginalised or minority patient populations	Systematic diagnostic error; unequal healthcare access; potential violation of equality norms	Bias audit mandates; diverse dataset requirements; regulatory fitness testing
Cybersecurity Vulnerability	Networked AI systems handling electronic health records and connected medical devices	Targeted ransomware; patient safety risks; institutional reputational harm	Mandatory security standards; breach notification duties; sector-specific cyber regulation
Institutional Accountability	Hospital and healthcare facility deployment of AI tools without adequate governance	Diffusion of responsibility; inadequate oversight; patient harm without remedy	Institutional AI governance policies; ethics committee review; liability attribution rules

Source: Based on WHO guidance on AI for health, NIST AI risk-management guidance, and peer-reviewed literature on clinical AI ethics, algorithmic bias, opacity, and data governance.[1,2,40,43 45,47 49]

Table 2. Comparative Regulatory Concerns in AI-Driven Healthcare

Jurisdiction	Data Protection Concern	Medical Liability Concern	Transparency Requirement	Patient Consent Concern
European Union	GDPR Article 9 treats health data as special-category data; Regulation (EU) 2025/327 establishes the European Health Data Space, with phased application.	The AI Act is in force and classifies certain medical-device AI as high-risk, but the relevant high-risk product rules are phased; the revised Product Liability Directive also requires national transposition.	The AI Act contains documentation, logging, human-oversight and post-market obligations for high -risk systems, subject to its phased application timetable.	GDPR Article 22 restricts certain solely automated decisions with legal or similarly significant effects and requires safeguards; this is distinct from clinical treatment consent.
United States	HIPAA governs protected health information; FTC Act applies to consumer health data; state-level frameworks vary	Traditional medical malpractice law applied to AI tools; FDA oversight of software as medical device (SaMD)	FDA's 2026 Clinical Decision Support Software guidance clarifies the scope of device oversight for CDS; other transparency practices also rely on guidance and standards.	Patient rights under HIPAA; state-based informed consent doctrine; no unified federal AI consent law
India	The DPDP Act 2023 uses a general personal-data framework rather than a separate "sensitive personal data" category; the Act and DPDP Rules 2025 have phased commencement.	Medical negligence remains governed by tort/consumer law and, where criminal negligence is alleged, the Bharatiya Nyaya Sanhita, 2023; there is no AI-specific liability statute.	NITI Aayog responsible-AI principles and ABDM governance are policy or sectoral instruments; there is no horizontal binding AI-transparency statute.	Clinical consent and personal-data consent are distinct; there is no AI-specific clinical-consent statute, and the DPDP framework was only partly commenced at the cut-off date.
United Kingdom	UK GDPR and Data Protection Act 2018 govern health data; ICO guidance on AI and data protection	Common law negligence applies; MHRA regulates AI as medical devices; no dedicated AI liability statute	MHRA, NICE and ICO provide sectoral guidance. The former AI Safety Institute was renamed the AI Security Institute in February 2025 and is not a healthcare regulator.	General consent principles under common law and NHS frameworks; no AI-specific consent statute

China	Personal Information Protection Law and specific health data regulation govern AI-related health data	Civil Code provisions; administrative regulations on AI healthcare; national AI governance norms	Algorithm-recommendation provisions and the 2023 Interim Measures for Generative AI impose governance duties within their respective scopes; neither instrument is healthcare-specific.	Data subject rights under PIPL; informed consent in clinical settings governed by existing health law

Source: Based on comparative analysis of EU, US, Indian, UK and Chinese AI, data-protection, medical-device and healthcare regulatory instruments.[12,13,15,18,23,25,28,31 39,61,62,69]

intersect tort, data protection, medical-device, equality, and healthcare-governance rules.[43 46]

Table 1 below summarises these key legal risks, their healthcare contexts, the specific risks they create, and the regulatory responses that have been proposed or implemented in the jurisdictions under examination.

Table 1 shows that healthcare-AI risks cut across consent, privacy, tort and product liability, equality, cybersecurity, and institutional governance. To avoid repetition, the detailed doctrinal implications of these categories are addressed in Section 4 rather than restated in the Results.[47 50]

Regulatory Issues in Comparison Between Jurisdictions

From a comparative standpoint, the five jurisdictions differ considerably in how they acknowledge, articulate, and mitigate the legal risks in question. Table 2 provides a systematic comparison of the five dimensions of regulatory concerns for each jurisdiction.

Table 2 demonstrates divergence in both legal form and regulatory maturity. The EU combines the GDPR, the AI Act, the Medical Devices Regulation, the adopted European Health Data Space Regulation, and a revised Product Liability Directive whose national transposition deadline had not yet expired by the cut-off date. The United States relies on HIPAA, FTC authority, FDA medical-device regulation, state law, and updated FDA CDS guidance. India has enacted the DPDP Act 2023 and DPDP Rules 2025, but commencement is phased and India still lacks healthcare-specific AI legislation. The UK relies on data-protection law, common-law duties, and MHRA/NICE/ICO guidance, while China combines PIPL and the Civil Code with binding algorithm and generative-AI measures. These instruments differ materially in legal force, and guidance or policy statements should not be treated as equivalent to binding statutes or regulations.[12,13,15,18,23,25,28,31 39,61,62,69]

Across the jurisdictions, health information receives heightened protection through different legal mechanisms. The EU and UK treat health data as special-category data; HIPAA protects defined protected health information in covered US contexts; China's PIPL treats medical-health information as sensitive personal

information; India's DPDP Act does not create a separate statutory category of sensitive personal data. The comparison therefore distinguishes data classification from the separate questions of clinical consent, automated-decision safeguards, medical-device oversight, and liability.[13,23,25,32]

Governance Flow for Responsible AI Use in Healthcare

Responsible governance of AI in healthcare extends beyond the identification and comparison of legal risks, requiring the development of a coherent process framework that sets out obligations at the intersection of the AI lifecycle and clinical practice and patient care. Figure 1 provides an example of a governance flow. It illustrates the governance requirements associated with the collection of data, the acquisition of informed consent from patients, the processing of data by AI, the review of data by clinicians, the communication of information to patients, the assessment of liability, and the provision of oversight by regulators. The framework demonstrates the legal protections and structures of the organization that are expected to be in place at each of the steps in the process.

The governance flow represented in Figure 1 shows that in the context of AI-supported healthcare, legal accountability is a continuous process rather than an isolated event that can be implemented at individual stages within a clinical pathway or data processing route. Each step in the flow represents a different combination of legal responsibilities and obligations. Data collection

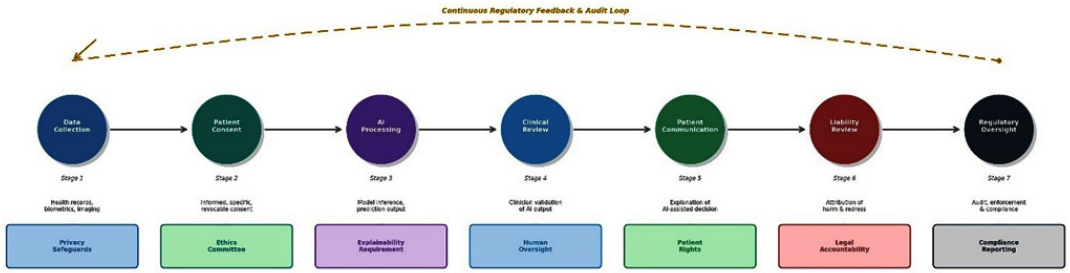


Fig. 1. Governance Flow for Responsible AI Use in Healthcare

Source: Based on WHO health-AI governance guidance, Indian responsible-AI principles, NIST AI RMF and ISO/IEC AI risk-management standards.[1,2,22,40 42]

	Design & Algorithm Safety	Deployment & Institutional Policy	Clinical Decision-Making	Data Privacy & Security	Transparency & Explainability	Harm Remediation & Redress
AI Developer / Manufacturer	Primary	Partial	—	Primary	Primary	Partial
Hospital / Healthcare Facility	Partial	Primary	Partial	Partial	Partial	Primary
Attending Physician	—	Partial	Primary	—	Partial	Partial
Data Processor	Partial	—	—	Primary	Partial	—
Regulatory Authority	Partial	Primary	—	Partial	Primary	Partial
Ethics Committee	—	Partial	Partial	Partial	Partial	Partial

Fig. 2. Legal Accountability Matrix for AI-Based Healthcare Decisions

Source: Based on peer-reviewed literature on medical AI liability and ethics, and public AI risk-governance standards.[29 31,40,41,51]

is subject to privacy and health data regulations. A patient's consent must be informed, specific, and revocable. AI must be processed with the assurance of quality, audits, and explainability. Clinical judgment is imperative to assess AI recommendations. Encompassing the AI elements of clinical encounters, patients must be informed, and liabilities must be assessed concerning all potential responsible parties. Regulatory oversight must employ a continuous loop of evaluation rather than a single-step approval process.

Legal Accountability Matrix for AI-Based Healthcare Decisions

Perhaps one of the most practically relevant issues facing the governance of AI within healthcare is the distribution of legal accountability for those involved in the design, implementation, and operation of AI systems. Figure 2 provides a legal accountability framework that illustrates the obligations and responsibilities for six actor classes across six accountability dimensions.

The accountability matrix in Figure 2 dispels the notion that any one actor can be assigned exclusive responsibility in any single dimension of accountability. AI developers are the primary actors regarding the safety and accuracy of the design of algorithms. However, the accountability matrix identifies shared responsibility for the transparency of algorithms and their deployment governance. This shared responsibility includes hospitals and the regulatory authorities. Primary responsibility for clinical decisions rests with the attending physician, who cannot be held accountable for flaws in the design of an algorithm. The primary responsibility of data processors is the data protection and security of that data. Regulatory authorities are primarily responsible for developing and enforcing a regulatory framework of compliance and oversight of institutional deployments. Ethics committees have shared responsibility in most of the dimensions of the accountability matrix, as they are advisory and oversee governance frameworks of institutions.

The distribution of responsibilities shown in Figure 2 supports a review of current and future legal reforms. Existing frameworks generally do not allocate responsibility ex ante across every actor and accountability dimension shown in the matrix; instead, responsibility is distributed among negligence, product-safety, data-protection, professional, and institutional rules. Accordingly, a clearer allocation of duties among developers, healthcare institutions, clinicians, data processors, and regulators is an important reform objective.

DISCUSSION

Special Legal Risks of Healthcare AI

When compared to the risks posed by other types of medical devices, the risks presented by healthcare-related AI systems are even more pronounced, and for several reasons. Traditional medical devices follow deterministic rules, and therefore, the output of these devices can be compared to standards of acceptable outputs. AI, however, outputs a result based on the training data and the organization of that data. It offers results that rely on the AI's training, the sample of the population to which the AI is applied, and the organization of that population. The lack of determinism present in AI systems greatly influences the traditional approach to medical negligence, which has considered the practice of medicine to a significant degree of professional reasonableness and the determinism of the medical practitioner.

Another distinctive risk is how AI may further existing inequalities in accessing and receiving healthcare. If the training data reviewed to develop an AI diagnostic system lacks representation of certain groups in society (defined by age, gender, ethnicity, and socieconomic/ geographic status), the system is likely to perform poorly when diagnosing those groups in comparison to well-represented groups. The resulting differences in clinical outcomes may make healthcare providers liable for claims of discrimination. Though the resulting differences in clinical outcomes may give rise to claims of discriminatory treatment under legislation that protects human rights, the legal frameworks may find it difficult to provide effective remedies since the causal mechanisms are complex. Most legal frameworks would be inadequate to address or detect differentiated harms that are demographic-specific because they analyze and focus primarily on safety and efficacy.[53,54]

AI systems are inherently adaptable and therefore pose particular legal risks. Machine learning models may be adjusted (retrained, or

modified) even after initial approvals, which may change how a system performs and impacts clinical outcomes in unfavorable ways. Legal frameworks and regulations that focus on medical devices or pharma may be unable to provide mechanisms for the continuous updating of AI systems. This risk is even more difficult to manage when the organizations that provide AI and healthcare products may offer and sell products rapidly (using a market first, evaluate later approach).

Informed Consent in AI-Assisted Clinical Settings

This piece of writing breaks consents into three groups. Clinical consent is for allowing an examination or treatment, and also for allowing the care provider to disclose pertinent information to the patient in the context of the care. For research consent, it is about the research participation. Consent for data processing is for the lawful data processing (if this is the lawful basis). Consent for one of these is distinct for the others.[26,52,58,64,65]

For clinical consent, AI involvement may be material when it substantially impacts the diagnosis or the treatment. So far, neither case (Montgomery v Lanarkshire Health Board [2015] UKSC 11) nor (Samira Kohli v Dr Prabha Manchanda [2008] 2 SCC 1) creates AI specific disclosure rules. So, it should be decided on a case to case basis whether AI should be disclosed, and should be decided based on clinical impact, law, and the information the patient should have to make an informed decision on the treatment.[64,65]

A related challenge is whether patients can understand the grounds and limits of an AI recommendation. Patients may have a right to relevant information for treatment even if a full technical explanation is not available. The clinically relevant explanation should be on the role of the AI, material limitations, uncertainty, and the availability of human review rather than on the assumption that patients should be able to access the model's internal technical explanation.

Data-processing consent is analytically distinct. In given circumstances, Health AI is able to process data on different legal bases. Consent is neither universally required nor universally sufficient. Under the GDPR, special categories of personal data require a legal basis in Article 6 and an applicable Article 9 condition. In India, the DPDP Framework provides for consent and certain legitimate uses, but at the time of the analysis, those provisions were in the process of being implemented. In addition to the DPDP Framework, Research uses would most likely be subject to statutory and ethics requirements.[13,23,26,58,61]

Algorithmic Opacity and the Right to Explanation

The GDPR does not establish an unlimited general right to a full technical explanation of every AI-assisted clinical output. Articles 13–15 require specified information about automated decision-making in relevant circumstances, while Article 22 addresses certain solely automated decisions producing legal or similarly significant effects. In Dun & Bradstreet Austria (Case C 203/22, 27 February 2025), the Court of Justice held that "meaningful information about the logic involved" requires information explaining, in a concise and intelligible way, the procedure and principles actually applied to reach the automated result. In healthcare, this data-protection duty should be distinguished from a clinician's separate obligation to explain diagnosis, risks, alternatives, and the role of AI in care.[13,27,63]

In the opacity challenge, the legal scholarship puts forth several potential solutions. These solutions range from the ex ante technical explainability requirement, which would formally mandate the interpretability of AI systems within high stake clinical domains, to the ex post explainability requirement, which would allow the interpretability of clinical AI systems on demand. The first solution, while more robust, could impose significant restrictions on the performance of AI systems. In contrast, the latter solution, while introducing less restriction, may not safeguard the interests of the data subject given that such explanatory tools are likely to produce post-hoc rationalizations of the model's decisions.

The explainability challenge becomes more complex because of the expertise needed to assess explanation of AI outputs. Even when technical explanations for AI outputs are available, their clinical and legal implications can only be evaluated by those who are both technically and contextually, in terms of the domain, knowledgeable. Therefore, the design of AI governance frameworks for healthcare should not only consider the technical aspect of the kinds of explanations that can be generated, but

also the institutional aspect of who possesses the capability as well as the legal authority to assess these explanations and transform them into legal and clinical actions.

Medical Liability and the Attribution of Responsibility

Ascertaining what the limits of legal liability should be in the case where harm results from AI-influenced medical choices is both an intellectually challenging and practically important question in the context of AI and the law. In most areas of law, the current legal regime of medical negligence is based on an individual account of the professional duty of care. This means that if an affected individual were to seek legal redress, a medical practitioner would be liable if the conduct of that practitioner fell below that of a reasonably skilled medical practitioner practicing in that specialty. The incorporation of AI systems into the practice of medical decision making creates a myriad of issues in that structure.

When a practitioner depends on an AI diagnostic system and it leads to the injury of a patient, the case for negligence must answer the following questions that existing law does not specify clearly. First, did the clinician's reliance on the AI output represent a deviation from the standard of reasonable care? Secondly, does the AI system (by itself) represent a separate harm? If so, who is to blame for this? Third, is it the case that the hospital that adopted the AI system had the responsibility to ensure that the AI System was safe and defendable in the scope of practice? Finally, did the AI developer have a responsibility to the patient who suffered injury as a result of the output from the AI system within the specified scope of care?

Faulty AI-enabled products may engage the principles of product liability against a manufacturer or developer. Directive (EU) 2024/2853 considers the liability of AI and is applicable to software. However, at the deadline for the submission of the text, the deadline for Member States to implement the Directive had not been reached. The Directive does not consider each erroneous probabilistic output as a product defect. Defectiveness of the product is fact-based and can exist alongside negligence, contract, regulatory, and institutional defects.[31]

The primary focus of this research is not whether AI should be considered a product defect to engage product liability, but rather what the emerging rules should be in the presence of other factors including design, implementation, reliance, data quality, and changes to the product post-market. The answer may differ depending on whether jurisdiction, the basis of the claim, and whether it is based on professional negligence, product liability, consumer remedy, contract, or a breach of a regulation.

The allocation of the problem to AI is illustrated by the Indian example. Civil medical-negligence claims continue to be pursued through the Consumer Protection Act 2019 and general principles of Tort, while the criminal negligence is under the recently enacted Bharatiya Nyaya Sanhita rather than the repealed Indian Penal Code. Jacob Mathew v State of Punjab, (2005) 6 SCC 1 remains the leading authority on medical negligence. The NMC's 2023 Registered Medical Practitioner (Professional Conduct) Regulations remain in abeyance, and the NMC continues to host the 2002 Code of Medical Ethics. Neither framework specifically allocates liability for AI-assisted clinical decisions. The DPDP Act 2023 is concerned with the processing of personal data and not a holistic regime for Healthcare-AI Liability.[23,55 57,66,67]

Institutional Accountability and Hospital Responsibility

In the context of clinical AI governance, hospitals, diagnostic laboratories, and integrated health systems play a unique role. Hospitals, as the decision-makers for purchasing, implementing, and managing operational AI systems, have a unique influence over the clinical applications of AI, separate from the technical obligations of AI developers and the ethical obligations of clinicians. The legal structures surrounding healthcare institutional responsibilities have typically concentrated on vicarious liability for the negligent acts of employed clinicians and direct liability for the deficits of internal governance and safety. Although the applied structures of institutional liability are relevant to AI governance, they still do not sufficiently address the specific challenges and risks that healthcare institutions face when AI is integrated into their operations.

Direct institutional accountability is therefore significant. Where a hospital procures

or deploys an AI clinical decision-support system without reasonable validation, staff training, escalation procedures, or monitoring, established principles of organisational or direct negligence may support liability, depending on the governing jurisdiction and the facts. This is an application of existing institutional duties to a new technology rather than a claim that a uniform AI-specific cause of action already exists.

Establishing policies and internal practices for AI procurement and deployment, ethics review and oversight of AI, reporting and review of incidents, and staff engagement and training demonstrates that an institution is committed to responsible AI governance. Numerous professional associations and regulatory bodies, as well as some countries, have begun to adopt governance structures in their AI regulatory frameworks. AI governance structures still remain in the early stages of implementation at a regulatory and legislative level.

Data Protection and Sensitive Health Information

The legal governance of healthcare AI places particular importance on health information. Health data often receives heightened protection, but not through an identical statutory category in every jurisdiction. The EU and UK designate health data as special-category data; US HIPAA protects defined protected health information in covered contexts; China's PIPL treats medical-health information as sensitive personal information; India's DPDP Act protects personal data generally and does not create a separate category of sensitive personal data. The practical scope and enforcement of these protections therefore differ.[13,23,25,32,59]

The protection of health data in the context of AI has some implications and challenges that current data protection laws may not be able to fully address. One concern is the re-identification risk. This refers to the risk of being able to identify individuals in un- or de-identified datasets as a result of using AI. This risk creates a real and persistent threat to patients' data privacy, even when that data has already been used to train an AI model. Another concern is the data protection principle of purpose limitation. This principle may be difficult to fulfill when data that was originally collected for clinical purposes, and subsequently used to train an AI model, is reused for research or commercial purposes. The treatment of such secondary reuse varies across jurisdictions and depends on the applicable legal basis, purpose-limitation rules, sectoral provisions, and research exceptions; uncertainty nevertheless persists in some AI-specific reuse scenarios.

AI can also intensify existing concerns involving genomic and biometric data. Genomic information can implicate biological relatives and raise group-privacy issues that individual consent models do not fully resolve. Biometric data may likewise create risks of reuse and function creep. These concerns are not outside all existing privacy law, but they illustrate limits in governance models that rely predominantly on individual notice and control.

Cybersecurity and Systemic Risk

The use of AI to automate healthcare introduces fundamental cybersecurity risks that have an impact on the safety of patients and the legal responsibility of providers. Autonomous connected healthcare devices, integrated electronic health record systems, AI diagnostic systems, and the hospital's network infrastructure are all vulnerable to an attack. Cybersecurity risks in healthcare are unique, as a cyberattack could result in not only the loss of confidential healthcare information, but also the manipulation of a healthcare AI's clinical AI decision systems, put the safety of patients at risk, or interrupt the operation of a clinical care device.

The cybersecurity regulations in the healthcare industry differ from region to region. There are regions that incorporate specific cybersecurity standards for healthcare businesses and medical device manufacturers during the approval or authorization for operations. Other regions create incentives for sufficient cybersecurity resources by utilizing general data protection and breach notification. A major concern for regulatory policy is whether the current regulations can address the complex threats that AI and healthcare cybersecurity presents.

Cyber incidents also complicate liability. Existing law can address parts of the chain through security duties, negligence, product liability, criminal law, and breach-notification rules, but attribution may remain difficult where multiple actors contribute to a patient-safety incident. Regulatory design should therefore combine proportionate security standards, incident

reporting, and clearer allocation of responsibility rather than assume that a single actor will always be legally responsible.

Bias, Discrimination, and Healthcare Inequality

From a legal and ethical perspective, one area of concern is the fact that AI applications in healthcare may create new problems, or make existing ones worse. As mentioned above, AI clinical tools may negatively affect the outcome and quality of healthcare services provided to certain demographic groups, depending on the demographic representation and the scope of the data considered when the tools are being developed. Inequality in the quality of diagnoses, treatment, and clinical outcomes can be considered a form of indirect discrimination. This discrimination is, in most of the jurisdictions analyzed, covered under the existing equality laws. However, the use of current equality laws to AI-generated healthcare inequities experiences some challenges, particularly in proof and causation, which legal scholarship still has not overcome.

The issue of AI system transparency is particularly challenging when trying to eliminate algorithmic discrimination in healthcare. In situations where discrimination takes place within a complex machine learning model, one may find it nearly impossible to prove that discrimination is a consequence of that specific AI model. Thus, from a legal and technical standpoint, it is challenging to establish regulations to support the principle of non-discrimination in healthcare algorithms and to require bias audits, demographic assessments, and performance assessments based on protected characteristics.

From a public healthcare governance standpoint, the inherent potential of AI systems to advance health inequities does not merely concern the individual rights of people affected by AI systems. In situations where AI systems in healthcare provide care of a poorer quality to disadvantaged groups, the systems will extend the gap in health equity that will be costly to individuals, communities, and healthcare systems. Consequently, the governance of AI in healthcare needs to balance social justice and individual rights. Regulations must incorporate health equity and the disproportionate population-level effects of AI use in healthcare.

Regulatory Gaps in India and Lessons from Other Jurisdictions

India is an interesting case when it comes to the connection between tech adoption and the ability to regulate. India is building an AI-driven healthcare system across the public and private sectors, operating electronic diagnostic and telemedicine systems and virtual health record systems. All this is happening while India incorporates regulatory frameworks that were created for the old, analog healthcare system, and which do not capture all of the legal issues that AI raises.

The DPDP Act 2023 is a horizontal data protection act that does not classify health data as sensitive data. It does not provide health-specific AI legislation. However, the DPDP Act 2023 is an important piece of legislation along with the DPDP Rules 2025 and accompanying measures. As of June 30, 2026, the framework was not completely in effect. There are gaps in theiac lifecycle, specifically regarding AI-specific transparency, validation, liability, and oversight.[23,53,61]

There are lessons India can learn from other countries' legislation. The EU's risk-based AI framework is one of those lessons, but the importance of the EU's Medical Devices Regulation framework, the GDPR, EHDS, and the phased approach to the AI Act must also be considered. India has the option to adopt a risk classification framework that has tiers for the validation, documentation, monitoring, and oversight of clinical systems. England has adopted an evidence-based framework that is worth considering.[60] Many of the frameworks are adopted through practice and not through a single, comprehensive piece of AI legislation. NITI Aayog, the National Health Authority, and medical device regulators can use these frameworks to guide the development of evidence-based, sector specific rules without treating other nation's legislation as directly permanently applicable.

Transparency, Auditability, and Human Oversight

The AI governance literature points to the principles of transparency, auditability, and human oversight as the rudimentary principles for responsible AI deployment in high-impact scenarios. In the case of healthcare, the principles

have specific legal and institutional dimensions that must be dealt with in a comprehensive governance structure.

Comprehensive transparency includes multiple facets: the acknowledgment of the role of AI in clinical decision making, clarity regarding the training data and limitations of the AI, and explication of the reasoning behind specific AI suggestions. These facets of AI transparency include various complexities and require a combination of different technologies, processes, and legal considerations. The acknowledgment of the role of AI in making clinical decisions is primarily an issue of ethics and informed consent. The clarity regarding training data and the limitations of the AI is largely an issue of compliance and regulatory reporting. The reasoning behind specific AI suggestions is primarily an issue of the right to justification in relation to administrative law and data protection.

Transparency and auditability go hand in hand. Transparency in AI systems means that sufficient information to evaluate the performance of the AI systems and the governance framework within which they operate is provided. Transparency and independent audits of the technical and regulatory aspects of AI systems in healthcare provide a safeguard to mitigate potential AI harms. An audit is a regulatory requirement of certain modern governance frameworks; however, they differ significantly with respect to the scope, independence, and frequency of the audits.

Human oversight recognizes that AI should complement and support rather than replace human judgment. The legal frameworks that articulate this principle vary. For example, some frameworks state that certain clinical decisions cannot be delegated to AI, while others state that AI's recommendations can only be acted on after a qualified clinician reviews and approves the recommendations. Setting the right balance of human oversight requirements is one of the more difficult types of AI regulatory challenges. If human oversight requirements are too strict, the AI productivity gains can be lost. On the other hand, if they are too lax, the potential exposure to serious patient safety concerns can become a reality.

The Role of Ethics Committees

Research ethics committees have a clearly established role where AI is studied through research involving human participants, including review of consent, privacy, equity, and risk-benefit issues. Their legal authority should not, however, be assumed to extend automatically to every routine clinical deployment of an AI tool outside a research protocol.[58]

For routine clinical AI, a hospital may use a multidisciplinary AI governance or ethics committee as an internal oversight mechanism, but such review is not a universal statutory prerequisite across the jurisdictions examined. Regulation should clarify when ethics or governance review is mandatory, advisory, or unnecessary, and how it relates to medical-device approval, data-protection compliance, clinical governance, and professional responsibility.

In addition to formal ethics committees, other mechanisms of ethical oversight, such as civil society organizations, professional regulatory bodies, and patient advocacy groups, have governance roles to play in the context of AI in healthcare. The development of governance structures which place a priority on patients and communities in the context of AI in healthcare is an important aspect of 'rights-based' AI governance which has been neglected in many of the existing frameworks.

Precautionary Principle, Patient Rights, and Innovation Balance

The precautionary principle is generally useful in high-risk clinical AI governance, but only to a certain extent. In Indian law, the Supreme Court has recognized its use mainly in environmental jurisprudence and in particular in the case of Vellore Citizens' Welfare Forum v Union of India, (1996) 5 SCC 647. This case is therefore an analogical usage and not as a direct application of environmental jurisprudence and clinical AI. Until there is certainty about the possible risks of causing serious and irreversible harm to patients, proportionate techniques may include procedures such as staged deployment, confirmation through validation, oversight, audits, and post market surveillance. This principle may be used in combination with risk-proportionality. For example, if the possible risk of clinical AI is greater, then more safeguards are appropriate, while if the risk is less, then the safeguards would be less burdensome.[68]

Maintaining the balance between patient rights and innovative advancements is a considerable challenge in AI governance. This balance must be met while ensuring patient protection and improving accessibility and efficiency of healthcare provided. Inadequate regulations have the potential to impose unjust costs on all stakeholders.

Risk-proportionality is useful to balance the aforementioned challenges. This approach maintains that as the potential risk to patients and the healthcare system increases, the legal safeguards must be more rigorous. Balancing this approach may allow for controlled and innovative advancements in clinical AI.

This approach will not constrain innovation. Innovation can thrive when rules about liabilities are clear and in proportion. Developers, clinicians, institutions, and patients will have greater clarity about the allowable scope of deployment. The focus is not for regulations to be as extensive as possible. The focus is on creating an appropriate framework that supports the development of positive healthcare AI.

CONCLUSION

This research focuses on AI within healthcare contexts to understand the issues of law, ethics, and policy regarding the protection of data, clinical accountability, consent, and transparency of algorithms. This research uses doctrinal and comparative methods of research within the EU, US, India, the UK, and China with a legal restriction of 30 June 2026. Biotechnology is only covered if it impacts clinical care or the governance of health data.

The outputs of some AI systems within healthcare could have a higher level of uncertainty than the outputs of most conventional medical technologies. Interpretable models of AI systems may exist, but healthcare systems may continuously evolve. Responsibility towards the provision of care is shared by developers, healthcare systems, clinicians, and data processors. These issues may amplify the risks of bias and disparities in healthcare that this technology may perpetrate.

No jurisdiction has a single comprehensive healthcare-AI code. The EU has the most developed combination of horizontal and sectoral instruments. These include the GDPR, AI Act, Medical Devices Regulation, EHDS, and the revised Product Liability Directive. Implementation is phased and healthcare obligations will remain dispersed across these instruments. Healthcare AI rules and transparency are also absent in phase-based frameworks like the US and India's DPDP. The UK and China primarily use sectoral laws and decisions and broad data and algotype regulations respectively, which are not targeted specifically at clinical AI.

Given these circumstances, this study will advance four concrete reforms instead of general rights that already exist. First, consideration should be given to the requirement of material disclosure of AI used in clinical care, the right to intelligible explanation and review in significant cases. Second, clarification of the liability allocation amongst the developers, the healthcare providers, and the clinical professionals should be considered. Third, governance of health data, particularly in India, should deal with re-identification, continuing processing, and the secondary use of training data. Fourth, a substantial governance system to include independent audits, incident review, and either ethics or governance oversight and involvement of the public should be put in place to control high-risk institutional deployments.

The proper management of AI in healthcare requires patient rights to be placed at the forefront, along with distribution of responsibility, fairness, and public accountability. Ensuring that all these considerations are legally protected requires the coordinated efforts of policymakers, health practitioners, and researchers, along with regulators and patient representatives.

ACKNOWLEDGEMENT

The authors would like to acknowledge the Department of Law, Manipal University Jaipur, for providing academic support and institutional resources for this research.

Funding Sources

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Conflict of interest

The authors do not have any conflict of interest.

Data Availability Statement

This statement does not apply to this article.

Ethics Statement

This research did not involve human participants, animal subjects, or any material that requires ethical approval.

Informed Consent Statement

This study did not involve human participants, and therefore, informed consent was not required.

Clinical Trial Registration

This research does not involve any clinical trials.

Permission to reproduce material from other sources

Not Applicable.

Author Contributions

Rahul Shamota: Conceptualization, Methodology, Formal Analysis, Writing Original Draft; Govind Yadav: Supervision, Validation, Writing - Review & Editing.

REFERENCES

1. World Health Organization. Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization; 2021. https://www.who.int/publications/i/item/9789240029200
2. World Health Organization. Regulatory considerations on artificial intelligence for health. World Health Organization; 2023. https://www.who.int/publications/i/item/9789240078871
3. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. OECD; 2019. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
4. UNESCO. Recommendation on the ethics of artificial intelligence. UNESCO; 2021. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence
5. Topol EJ. High-performance medicine: the convergence of human and artificial intelligence. *Nat Med*. 2019;25(1):44-56. https://pubmed.ncbi.nlm.nih.gov/30617339/
6. Esteva A, Kuprel B, Novoa RA, et al. Dermatologist-level classification of skin cancer with deep neural networks. *Nature*. 2017;542(7639):115-118. https://www.nature.com/articles/nature21056
7. Gulshan V, Peng L, Coram M, et al. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *JAMA*. 2016;316(22):2402-2410. https://pubmed.ncbi.nlm.nih.gov/27898976/
8. McKinney SM, Sieniek M, Godbole V, et al. International evaluation of an AI system for breast cancer screening. *Nature*. 2020;577(7788):89-94. https://pubmed.ncbi.nlm.nih.gov/31894144/
9. De Fauw J, Ledsam JR, Romera-Paredes B, et al. Clinically applicable deep learning for diagnosis and referral in retinal disease. *Nat Med*. 2018;24(9):1342-1350. https://pubmed.ncbi.nlm.nih.gov/30104768/
10. Jumper J, Evans R, Pritzel A, et al. Highly accurate protein structure prediction with AlphaFold. *Nature*. 2021;596(7873):583-589. https://www.nature.com/articles/s41586-021-03819-2
11. Vamathevan J, Clark D, Czodrowski P, et al. Applications of machine learning in drug discovery and development. *Nat Rev Drug Discov*. 2019;18(6):463-477. https://pubmed.ncbi.nlm.nih.gov/30976107/
12. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. *Off J Eur Union*. 2024;L:1-144. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
13. European Parliament and Council. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Off J Eur Union*. 2016;L119:1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
14. European Parliament and Council. Regulation (EU) 2017/745 on medical devices. *Off J Eur Union*. 2017;L117:1-175. https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng
15. European Parliament and Council. Regulation (EU) 2025/327 of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Off J Eur Union*. 2025. https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng
16. U.S. Food and Drug Administration. Artificial Intelligence/Machine Learning (AI/ML)-based software as a medical device (SaMD) action plan. FDA; 2021. https://www.fda.gov/media/145022/download
17. U.S. Food and Drug Administration. Proposed regulatory framework for modifications to artificial intelligence/machine learning-based software as a medical device. FDA; 2019. https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf

18. U.S. Food and Drug Administration. Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff. FDA; January 29, 2026. https://www.fda.gov/media/109618/download
19. International Medical Device Regulators Forum. Software as a medical device (SaMD): key definitions, IMDRF/SaMD WG/N10FINAL:2013. IMDRF; 2013. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf
20. International Medical Device Regulators Forum. Software as a medical device (SaMD): clinical evaluation, IMDRF/SaMD WG/N41FINAL:2017. IMDRF; 2017. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-170921-samd-n41-clinical-evaluation_1.pdf
21. NITI Aayog. National strategy for artificial intelligence #AIforAll. Government of India; 2018. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
22. NITI Aayog. Responsible AI for all: approach document for India, part 1 - principles for responsible AI. Government of India; 2021. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
23. Government of India. The Digital Personal Data Protection Act, 2023. Ministry of Law and Justice; 2023. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
24. National Health Authority. Health Data Management Policy. Government of India; 2020. Revised 2022. https://abdm.gov.in/strapicms/uploads/HDM_Press_Release_48807ee0b7.pdf
25. U.S. Department of Health and Human Services. Standards for privacy of individually identifiable health information, 45 CFR Parts 160 and 164. HHS; 2002. https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information
26. European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679. EDPB; 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
27. Article 29 Data Protection Working Party. Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP251 rev.01. European Commission; 2018. https://ec.europa.eu/newsroom/article29/items/612053/en
28. Information Commissioner's Office. Guidance on AI and data protection. ICO; 2020. Updated March 15, 2023. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
29. Price WN II, Gerke S, Cohen IG. Potential liability for physicians using artificial intelligence. *JAMA*. 2019;322(18):1765-1766. https://pubmed.ncbi.nlm.nih.gov/31584609/
30. Cohen IG, Amarasingham R, Shah A, Xie B, Lo B. The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Aff (Millwood)*. 2014;33(7):1139-1147. https://pubmed.ncbi.nlm.nih.gov/25006139/
31. European Parliament and Council. Directive (EU) 2024/2853 of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. *Off J Eur Union*. 2024. https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng
32. Standing Committee of the National People's Congress. Personal Information Protection Law of the People's Republic of China. NPC; 2021. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
33. Standing Committee of the National People's Congress. Data Security Law of the People's Republic of China. NPC; 2021. https://en.spp.gov.cn/2021-06/10/c_948426.htm
34. Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration for Market Regulation. Provisions on the Administration of Algorithmic Recommendation in Internet Information Services. 2021; effective March 1, 2022. https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm
35. Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, et al. Interim Measures for the Management of Generative Artificial Intelligence Services. 2023; effective August 15, 2023. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
36. Department for Science, Innovation and Technology. A pro-innovation approach to AI regulation. HM Government; 2023. https://assets.publishing.service.gov.uk/media/64cb71a547915a00142a91c4/a-pro-innovation-approach-to-ai-regulation-amended-web-ready.pdf
37. Medicines and Healthcare products Regulatory Agency. Software and AI as a medical device change programme: roadmap. MHRA; 2021. Updated 2023. https://www.gov.uk/government/

publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap

38. National Institute for Health and Care Excellence. Evidence standards framework for digital health technologies. NICE; 2022. https://www.nice.org.uk/what-nice-does/digital-health/evidence-standards-framework-esf-for-digital-health-technologies
39. U.S. Food and Drug Administration. Marketing submission recommendations for a predetermined change control plan for artificial intelligence-enabled device software functions: guidance for industry and FDA staff. FDA; 2025. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence
40. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST; 2023. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
41. International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 23894:2023 artificial intelligence - guidance on risk management. ISO; 2023. https://www.iso.org/standard/77304.html
42. International Organization for Standardization and International Electrotechnical Commission. ISO/IEC 42001:2023 information technology - artificial intelligence - management system. ISO; 2023. https://www.iso.org/standard/42001
43. Char DS, Shah NH, Magnus D. Implementing machine learning in health care: addressing ethical challenges. *N Engl J Med*. 2018;378(11):981-983. https://pubmed.ncbi.nlm.nih.gov/29539284/
44. Rajkomar A, Hardt M, Howell MD, Corrado G, Chin MH. Ensuring fairness in machine learning to advance health equity. *Ann Intern Med*. 2018;169(12):866-872. https://pmc.ncbi.nlm.nih.gov/articles/PMC6594166/
45. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*. 2019;366(6464):447-453. https://pubmed.ncbi.nlm.nih.gov/31649194/
46. Rumbold JMM, Pierscionek BK. The effect of the general data protection regulation on medical research. *J Med Internet Res*. 2017;19(2):e47. https://www.jmir.org/2017/2/e47/
47. Price WN II. Big data and black-box medical algorithms. *Sci Transl Med*. 2018;10(471):eaao5333. https://pmc.ncbi.nlm.nih.gov/articles/PMC6345162/
48. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L. The ethics of algorithms: mapping the debate. *Big Data Soc*. 2016;3(2):1-21. https://journals.sagepub.com/doi/10.1177/2053951716679679
49. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *Int Data Priv Law*. 2017;7(2):76-99. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469
50. Floridi L, Cowls J, Beltrametti M, et al. AI4People: an ethical framework for a good AI society. *Minds Mach*. 2018;28(4):689-707. https://link.springer.com/article/10.1007/s11023-018-9482-5
51. Gerke S, Minssen T, Cohen IG. Ethical and legal challenges of artificial intelligence-driven healthcare. In: Bohr A, Memarzadeh K, eds. *Artificial Intelligence in Healthcare*. Academic Press; 2020:295-336. https://pmc.ncbi.nlm.nih.gov/articles/PMC7332220/
52. World Medical Association. World Medical Association Declaration of Helsinki: ethical principles for medical research involving human subjects. *JAMA*. 2013;310(20):2191-2194. https://pubmed.ncbi.nlm.nih.gov/24141714/
53. Government of India. Medical Devices Rules, 2017. Ministry of Health and Family Welfare; 2017. https://cdsco.gov.in/opencms/resources/UploadCDSCOWeb/2022/m_device/Medical%20Devices%20Rules,%202017.pdf
54. Board of Governors in Supersession of Medical Council of India. Telemedicine practice guidelines: enabling registered medical practitioners to provide healthcare using telemedicine. Ministry of Health and Family Welfare; 2020. https://pmc.ncbi.nlm.nih.gov/articles/PMC8106416/
55. Government of India. The Consumer Protection Act, 2019. Ministry of Law and Justice; 2019. https://ncdrc.nic.in/bare_acts/CPA2019.pdf
56. Government of India. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), in force from July 1, 2024. India Code. https://www.indiacode.nic.in/handle/123456789/20062
57. Medical Council of India. Code of Medical Ethics Regulations, 2002. National Medical Commission. https://www.nmc.org.in/rules-regulations/code-of-medical-ethics-regulations-2002/
58. Indian Council of Medical Research. National ethical guidelines for biomedical and health research involving human participants. ICMR; 2017. https://ethics.ncdirindia.org/asset/pdf/ICMR_National_Ethical_Guidelines.pdf
59. Council of Europe. Protocol amending the Convention for the Protection of Individuals with

regard to Automatic Processing of Personal Data, CETS No. 223. Council of Europe; 2018. https://www.riigiteataja.ee/aktilisa/2030/7202/0002/ETS_No.pdf

60. NHSX. A guide to good practice for digital and data-driven health technologies. Department of Health and Social Care; 2021. https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology
61. Ministry of Electronics and Information Technology. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025. Government of India. https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
62. Department for Science, Innovation and Technology. Tackling AI security risks to unleash growth and deliver Plan for Change: UK AI Safety Institute becomes UK AI Security Institute. UK Government; February 14, 2025. https://www.gov.uk/government/news/tackling-ai-security-risks-to-unleash-growth-and-deliver-plan-for-change
63. Court of Justice of the European Union. Dun & Bradstreet Austria GmbH v Magistrat der Stadt Wien, Case C-203/22, Judgment of 27 February 2025, ECLI:EU:C:2025:117. https://curia.europa.eu/juris/document/document.jsf?docid=295841&doclang=en
64. UK Supreme Court. Montgomery v Lanarkshire Health Board [2015] UKSC 11; [2015] AC 1430.
65. Supreme Court of India. Samira Kohli v Dr Prabha Manchanda & Anr, (2008) 2 SCC 1; 2008 INSC 56.
66. Supreme Court of India. Jacob Mathew v State of Punjab & Anr, (2005) 6 SCC 1.
67. National Medical Commission. Notification placing the National Medical Commission Registered Medical Practitioner (Professional Conduct) Regulations, 2023 in abeyance. 24 August 2023. https://www.nmc.org.in/ActivitiWebClient/open/get Document?path=%2 FDocuments%2F Public%2FPortal%2FNmcGazette%2F248297.pdf
68. Supreme Court of India. Vellore Citizens' Welfare Forum v Union of India, (1996) 5 SCC 647.
69. U.S. Food and Drug Administration. Clinical Decision Support Software: Frequently Asked Questions (FAQs). FDA; June 29, 2026. https://www.fda.gov/medical-devices/software-medical-device-samd/clinical-decision-support-software-frequently-asked-questions-faqs