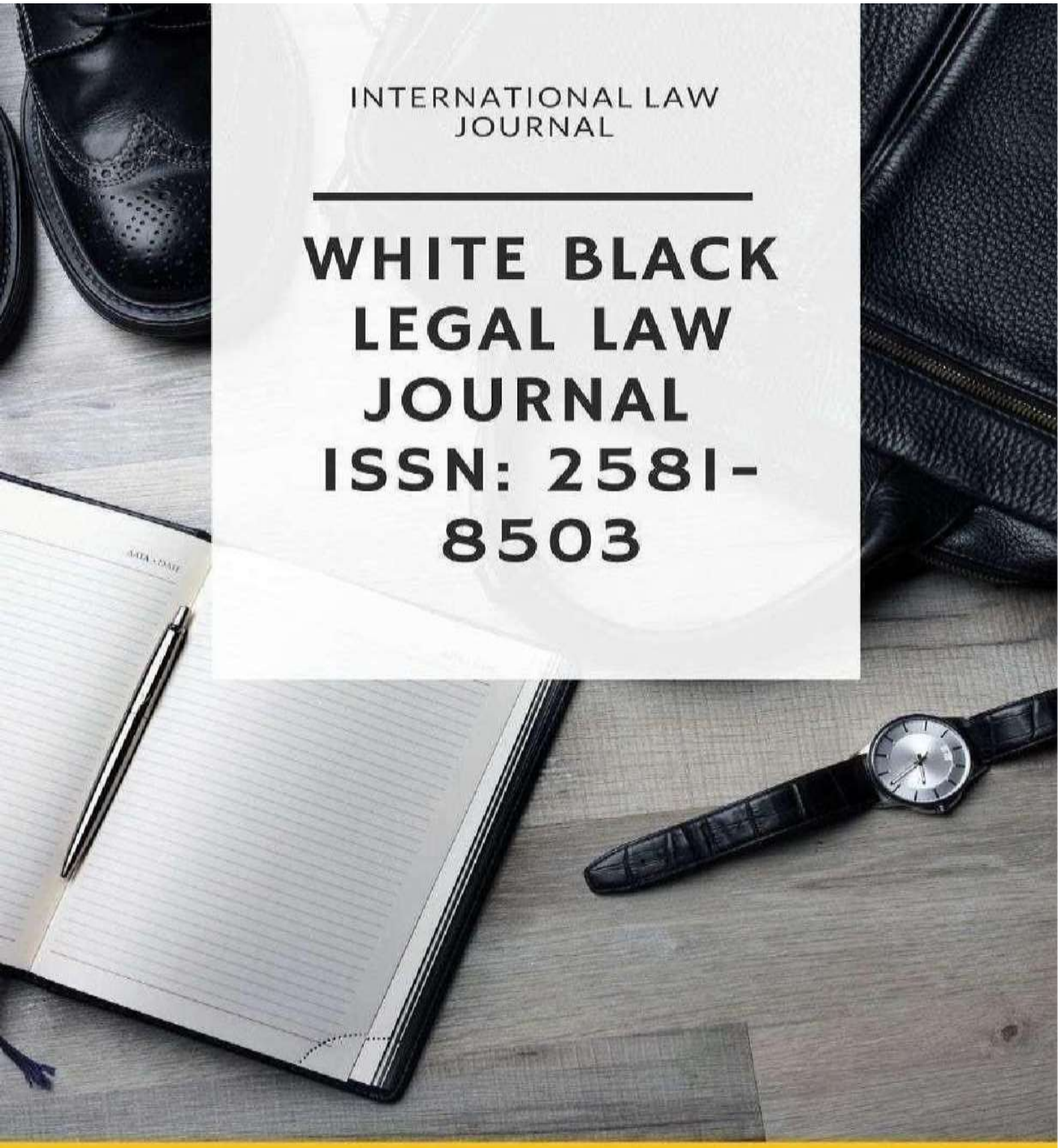

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | May 2025 ISSN: 2581-8503

PRIVACY RISKS & CHALLENGES IN AI-DRIVEN HEALTHCARE SYSTEMS

AUTHORED BY - BHAVYA SHEETAL
University: Amity University, Noida

DATA TRANSPARENCY & EXPLAINABILITY ACROSS JURISDICTIONS

As AI systems increasingly play a key role in health care delivery, the issues of data transparency and explainability have emerged as central themes of legal & ethical discourse. These principles are necessary to ensure that patients and practitioners understand how AI systems process data & come to clinical decisions. Transparency encompasses the disclosure of information regarding data collection as well as use & sharing, whereas explainability describes the ability of AI models to generate human-comprehensible explanations for their outputs. This section examines how these imperatives are addressed by transformed legal regimes, especially in the EU, US, & Indian contexts, showing similarities and differences in dominant modes of governance in global healthcare.[1]

The Legal Foundations of Transparency & Explainability

Transparency & add transparency add relation serve not only instrumental but also intrinsic role in the medicine. Instrumentally, they enable patients to make informed choices, promote auditability of AI systems, & enable redress in case of mistakes. They do so by preserving human agency over decisions related to their own well-being, thus preserving individual dignity & autonomy. These concepts have increasingly received recognition in legal systems where the use of AI to predict risk, diagnose, & recommend treatment has been deployed. Nonetheless, their legally actionable power differs greatly from one jurisdiction to another.[2]

European Union: Leading the Rights-Based Approach

In terms of data transparency & explainability for the AI-driven healthcare, the GDPR

[1] Brent Mittelstadt et al, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3(2) Big Data & Society 1.
[2] Sandra Wachter, 'Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, & the GDPR' (2018) 34(4) Computer Law & Security Review 436.

provides the most sophisticated & enforceable legal framework. The principle of lawfulness, fairness, and transparency is outlined in Article 5 of the GDPR, whereas Article 13 mandates that data controllers must notify data subjects about the logic underlying automated processing. Importantly, Article 22 establishes the right to not be subjected to subjected to solely automated decision-making, including profiling, that has legal or similarly significant effects. There is an ongoing discussion whether the art. 22 GDPR demands a right to explanation, but the EDPB has already made clear that "meaningful information about the logic involved" must still be given to affected persons. This is especially pertinent in medical situations, in which the algorithmic decisions may be related to diagnoses, or courses of treatment. Alongside GDPR, The EU's Ethical Guidelines for Reliable AI emphasize the importance of transparency, accountability & human oversight as foundational principles. Such soft-law instruments affect the way that member states assess compliance with AI technologies.[3]

United States: Fragmented & Sectoral Frameworks

In contrast, the U.S. does not have a comprehensive data protection law & relies on sectoral laws like the HIPAA & FDA oversight. HIPAA protects the confidentiality & security of PHI but does not address how to explain AI models. Most recently, the FDA released guidance in the use of AI/ML-based *"Software as a Medical Device (SaMD)"*, & urged developers to integrate GMLP; principles that would essentially codify documentation & transparency of algorithms. However, despite these efforts, there are currently no binding legal obligations on healthcare providers or AI developers to achieve understanding of decision-making by patients. The Algorithmic Accountability Act — which, while introduced in Congress, has not been passed yet however — aims to mandate requirements for companies deploying what are called high-impact algorithms, from conducting impact assessments to being transparent. Until such laws are enacted, the US is dependent on voluntary standards & professional ethics.[4]

India: Emerging but Limited Provisions

India's new DPDP Act adopts a consent-based legislation for data handling, but provides minimal prescriptive guidance around transparency & explainability. Although the Act requires Data Fiduciaries to provide individuals with details regarding the personal information that is being gathered, the purpose & nature of data collection, it does not require that individuals

[3] European Data Protection Board, Guidelines on Automated Individual Decision-Making & Profiling (2018).
[4] US Food & Drug Administration, Proposed Regulatory Framework for Modifications to AI/ML-Based Software as a Medical Device (2021).

understand algorithmic logic or automated decision-making processes. Still, evolution is afoot. The NDHM & ABDM frameworks promote transparency in health data governance, including policies around data sharing & individual access rights. NITI Aayog of India also released their Principles for Responsible AI, which are recommendations that emphasize similar principles such as transparency, explainability, & auditability of AI systems. Without binding obligations, Indian patients may be left uninformed about the reasoning underpinning AI systems in healthcare & how they arrive at conclusions or recommendations, particularly in privately developed tools.[5]

Technical & Practical Barriers

Transparency & explainability have technical challenges as well, especially for "black box" models like deep neural networks. These systems provide little interpretability intrinsically, rendering it challenging for developers to understand the reasoning behind their choices.[6]

Post hoc methods have been developed as part of efforts to enhance explainability, in the form of LIME & SHAP, which provide probabilistic approximations of model behaviour. However, these tools are not always accurate nor layperson understandable, which limits their clinical usability. There is a balance to be struck between interpretability and performance. Models that are extremely accurate are frequently less explainable, leading to ethical concerns as to whether better clinical outcomes can justify the loss of explanations—especially at the risk of patient autonomy.[7]

Ethical & Human Rights Dimensions

There is an increasing appreciation of transparency and explainability through a human rights lens, notably in the EU, where the principles are connected to the right to privacy & non-discrimination. These links have been strengthened by the Council of Europe's Convention 108+ & the European Court of Human Rights. In contrast, these principles are typically framed in the language of consumer protection or due process in jurisdictions like the US & India, focusing to some extent on a limited form of consumer protection or user due process, & thus rendering them much lower in terms of their normative force (Markus, 2022, Moore, 2019). This difference mutualizes the brumous of international cooperation & the barter of health data

[5] National Health Authority (India), Ayushman Bharat Digital Mission: Health Data Management Policy (2020).
[6] Finale Doshi-Velez & Been Kim, 'Towards A Rigorous Science of Interpretable Machine Learning' (2017) arXiv:1702.08608.
[7] Marco Tulio Ribeiro et al, '"Why Should I Trust you?": Explaining the Predictions of Any Classifier' (2016) Proceedings of the 22nd ACM SIGKDD 1135.

governance, incites cross-border use of an opaque beleab in land of accounting beamed in jurisdictions with delicate accountability standards.[8]

Data transparency & explainability are at the core of the ethical & legal sound deployment of AI in healthcare. While the EU has laid down these principles clearly in law, in the US & India, it is sectoral or soft-law instruments that are relied on, leading to fragmented & uneven protections. As AI systems shape clinical decision-making, global harmonisation of transparency standards that leaves no room for wiggle room or interpretation — supported by redressable statutory obligations — is vital. Such harmonisation shall not just safeguard patient rights but also builds trust & legitimacy in AI empowered healthcare.

RISKS OF ALGORITHMIC BIAS: LEGAL PROTECTIONS IN VARIOUS COUNTRIES

The potential of Artificial Intelligence (AI) to modify clinical practice, improving diagnoses & many health outcomes. Yet, with such benefits come the risk of algorithmic bias, systemic & often unintended errors in machine learning models that can disproportionately impact groups of people, resulting in discrimination. These kinds of biases can come from biased or incomplete datasets, problems with the design of an algorithm, or not properly testing a model. The implications of such bias are especially dire in health care, where they may manifest as disparities in diagnosis, treatment, & health outcomes. This section explores the approaches taken by legal systems to Algorithmic Bias in AIs, with an emphasis on health applications, in the EU, the US & India.[9]

European Union: Regulatory Precision & Proactivity

The European Union has established itself as a worldwide frontrunner in ethical & rights-based AI laws. The EU's response to algorithmic bias is grounded in two complementary legal instruments: the GDPR & the proposed AI Act.

- **GDPR:** The GDPR, effective since 2018, provides a foundation for addressing algorithmic bias through several core provisions:
  - Article 22 forbids making decisions that rely entirely on automated processes, including profiling, which lead to legal or similarly important consequences for individuals, unless safeguarded by explicit consent or authorized by law.

[8] Council of Europe, Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), 2018.
[9] Brent Mittelstadt, Chris Russell & Sandra Wachter, 'Explaining Explanations in AI' (2019) 3(1) Fat 279.

- Recital 71 underscores the importance of protecting individuals from discriminatory effects caused by profiling, especially based on delicate personal information such as health, ethnicity, or gender.

Together, these provisions place a requirement for data controllers to establish sufficient actions to guarantee fairness, transparency, and non-discrimination in processes involving automated decision-making.

- **Proposed AI Act:** Introduced in 2021, the Artificial Intelligence Act categorizes AI technologies employed in healthcare as "high-risk", imposing strict regulations on them. regulatory oversight. Key obligations include:
  - Risk Management: Developers must implement a risk management system that includes pre-market testing & post-deployment monitoring.[10]
  - Data Governance: The Act mandates the use of high-quality, representative, & bias-free datasets for the purpose of training, validating, and testing AI systems.
  - Transparency & Human Oversight: Developers must provide detailed documentation & ensure human oversight to mitigate bias & facilitate accountability.

This legislation is the most extensive attempt to mitigate algorithmic bias at the legislative level, reflecting the EU's broader human rights-centric approach to digital governance.

USA: Sectoral Regulation & Fragmented Progress

The United States lacks an all-encompassing federal statute addressing algorithmic bias in AI, unlike the E.U. Instead, its response is patchwork, with laws that are either sector specific or state level & vary in maturity, leaving many regulatory gaps that states are racing to fill.

- **HIPAA & Healthcare Regulation:** The HIPAA is a central1 law with strong protections for data confidentiality & safety, & guards against algorithmic bias, but HIPAA does not specifically address AI accountability and algorithmic bias in healthcare. The FDA has a regulatory role in reference to the approval of AI-enabled medical devices, but it mainly investigates safety & effectiveness, not fairness or bias.
- **Federal Guidance & Initiatives:** Although enforcement at the federal level has been low so far, recent events are symptomatic of a growing concern about bias:

[10] European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM (2021) 206 final.

- The EEOC has cautioned employers about the risk of algorithmic discrimination in workplace health monitoring.[11]
- The suggested Algorithmic Accountability Act has not yet been enacted into law, would force companies to audit their automated systems for risk, including bias & discrimination.[12]

- **State-Level Innovations:** Some US states have passed new laws to counter algorithmic bias:
  - Illinois passed the AI Video Interview Act, mandating that employers reveal the utilization of artificial intelligence in hiring & safeguarding data.[13]
  - New York City mandates annual bias audits for automated hiring tools, which may encompass AI systems that screen candidates for health-related job suitability.[14]
  - The Colorado AI Act, which also applies to gen AI, requires companies that use AI systems with high levels of risk in areas like healthcare to provide annual assessments of the impact of their systems for bias, discrimination & safety.[15]

But between these promising steps, there remains considerable uncertainty & variation in protections because of the lack of a unified federal framework.

India: Early-Stage Development & Policy-Driven Approach

Algorithmic bias in India's regulatory landscape is still evolving. The standard data security law of the country, DPDP Act does not have specific provisions to address bias in AI systems.

- **Policy Guidelines:** NITI Aayog, the public policy think tank of India, has laid down the Responsible AI guidelines, which centre fairness, transparency, & inclusivity as key guiding principles. But there are guidelines that simply don't have the legal teeth to hold developers responsible for biases in outcomes.[16]
- **Healthcare Regulatory Context:** India's infection of digital health platforms & AI tools through policies like the Ayushman Bharat Digital Mission offers opportunities but also carries risks. Without sector-specific legal standards to guide against bias in the use of AI systems, vulnerable populations will fall prey to discriminatory practices in resource-limited settings.[17]

[11] US EEOC, Enforcement Guidance on Harassment in the Workplace (2024).
[12] Algorithmic Accountability Act, HR 6580, 117th Congress (2022).
[13] Illinois Compiled Statutes, 820 ILCS 42/ (Artificial Intelligence Video Interview Act).
[14] New York City Local Law No. 144 of 2021.
[15] Colorado Senate Bill 24-205 (2024).
[16] NITI Aayog, Responsible AI for All: Discussion Paper (2021).
[17] Ayushman Bharat Digital Mission, Health Data Management Policy (2020).

Comparative Insights & Global Outlook

JURISDICTION	LEGAL PROTECTION AGAINST ALGORITHMIC BIAS
EU	Strong protection under GDPR & AI Act, with specific obligations for high-risk healthcare AI.
US	Patchwork of sectoral regulations; some states advancing bias audits & accountability mechanisms.
INDIA	Early-stage legal development; existing protections are policy-driven & non-binding.

The uneven regulation of algorithmic bias is emblematic of larger differences in legal nerd cultures, regulatory capacity, & societal priorities around the world. With AI technologies ever more transnational, there is an urgent need for international collaboration to develop coordinated norms that can guarantee that these new kinds of systems are equitable & accountable across geographical domains. A major threat for fairness & equity in AI systems in healthcare is algorithmic bias. While the European Union has instituted a well-established regulatory framework to mitigate this risk, the United States & India still high varieties of legal maturation. The answer: a multi-tiered approach—legal, technical, ethical, & data-driven—to bar the prospect that AI systems would replicate, if not worsen, health disparities. Moving forward successfully will require international cooperation, flexible regulations, & a steadfast dedication to maintaining patient dignity in the digital world.

VARIABILITY IN CONSENT STANDARDS (INDIA VS EU VS US)

Consent is one of the ethical & legal cornerstones of data processing in health care. It entails respect for patient autonomy & provides a key means by which individuals should have authority over their personal information. Nonetheless, the methods for enhancing and safeguarding consent vary significantly across different regions, particularly in India, the EU, and the US. These variations arise from contrasting legal traditions and regulatory systems, & cultural attitudes toward privacy and autonomy. Here we analyse all three of these areas in terms of the differences in the scope of consent frameworks for healthcare & AI systems across the three regions.

European Union: Gold Standard of Explicit & Informed Consent

The EU's GDPR, in effect since 2018, the world's gold standard for consent standards around

data processing. The handling of personal information, particularly sensitive categories such as health data, is governed by Article 6 and Article 9 of the GDPR, which mandates that there must be a legitimate reason for processing — explicit consent being one of the most invoked justifications. Key Features of GDPR Consent:

- Freely Given: Consent cannot be obtained under duress.
- Informed — Individuals should have complete knowledge of the data being gathered, including its intended use, how it will be utilized, and the entities with whom it will be shared.
- Specific and Unambiguous: General or blanket consent is ineffective. Consent must be separate & clearly delineated for each purpose of processing.
- Right to Withdraw: Individuals must be able to revoke their permission at any time, & it needs to be as burdensome to withdraw as it was to provide.

The GDPR also imposes transparency obligations (Articles 13 & 14) & requires data controllers to provide comprehensive privacy notice using plain & intelligible language. In a healthcare setting, particularly with AI-powered diagnostics & predictive systems, these standards allow patients to be aware of the implications of automated data processing. The GDPR also mandates greater safeguards for consent in automatic decision making & profiling (Article 22) as necessity, human intervention, responses, & explanations where AI impacts medical decisions.[18]

United States: Implied & Institutional Consent Frameworks

The United States employs a more fragmented, sector-specific strategy regarding data privacy, where consent in the health care space is primarily dictated by the HIPAA. Important Aspects of HIPAA Consent:

- Implied Consent for Essential Operations: HIPAA gives practitioners authorization to utilize and share patient health information for the purposes of treatment, payment, and healthcare operations without the need for a signed patient consent.
- Secondary Use Authorization: Written patient authorization is generally required for research, marketing, or data sharing with third parties outside of the core activities of care.
- Notice of Privacy Practices (NPP) — A healthcare provider has to provide an NPP that tells the patient how his (or her) data will be used. However, you acknowledge receipt of this notice is not a condition of receiving care & does not equate to formal consent.

[18] Regulation (EU) 2016/679 (General Data Protection Regulation), arts 6, 9, 13, 14, 22.

This framework is much more about regulatory compliance than patient empowerment. A level of institutional trust lies at the centre of the HIPAA framework, placing the onus of data protection on covered entities & business associates. A major limitation is the narrow scope of HIPAA. Most emerging digital health technologies — such as fitness trackers, Ai-based health apps & telehealth tools not associated with traditional health care providers — are not covered by HIPAA, leading to variations in consent practices. Moreover, US law does not require granular consent for different types of processing, nor easy withdrawal of consent in all contexts.[19]

India: Emerging Consent Norms under the DPDP Act

The DPDP Act establishes a comprehensive legal framework governing data privacy in India with a focus on consent-based processing. The Act was enacted in the aftermath of the landmark Supreme Court judgement in *Justice K.S. Puttaswamy v Union of India*, which had held privacy to be a fundamental right. Key Features of DPDP Consent:

- Free, Informed, Specific, & Unambiguous: Following the language of the GDPR, the Act requires that consent be clear & derived from an understanding of the use of any data.
- Notice Requirement: Data Fiduciaries are mandated to furnish a clear, concise notice regarding the characteristics and intent behind the handling of personal information during the moment it is gathered.
- Right to Withdraw: Individuals (Data Principals) have the ability to revoke their consent at any given time, and there should be systems established to make this process easier.
- No Processing Without the Consent: Under the DPDP Act consent is the default legal basis so no processing is permitted unless it is for legitimate use cases like medical emergencies & public interest.

Yet the Act fails to class health data as "sensitive", nor does it offer any provisions specifically dealing with AI or automated decision making. Also, the absence of rich procedural safeguards designed around granular consent raises questions about how adaptable it may be to dynamic data spaces, including AI-based systems in health care.

[19] Nicolas P Terry, 'Protecting Patient Privacy in the Age of Big Data' (2014) 81(2) UMKC Law Review 385.

Comparative Analysis & Challenges in Practice

FEATURE	EU (GDPR)	US (HIPAA)	INDIA (DPDP ACT)
CONSENT TYPE	Explicit, informed, granular	Implied for care; explicit for others	Explicit, informed, default basis
CONSENT WITHDRAWAL	Mandatory & easy	Not uniformly required	Mandatory, process to be specified
APPLICABILITY	All sectors & entities	Sector-specific (healthcare)	All digital personal data
COVERAGE OF AI	Some provisions (Article 22)	No specific AI coverage	No direct AI or profiling regulation
PROTECTION OF HEALTH DATA	Special category with higher safeguards	Protected health info (PHI)	No special categorisation yet

In most jurisdictions, one of the biggest difficulties is regarding the practical application of consent. Many consent forms are overly wordy, overly legalistic or even vaguely worded — undermining the very idea of "informed" consent. In the context of algorithms that might change over time, dynamic or tiered consent becomes necessary but is rarely practiced in related AI systems. Consent continues to be a key principle in data protection regimes, however its conceptualisation & application differ greatly between jurisdictions. The EU has the strongest & most individual-oriented model of personal data governance globally, establishing the gold standard for informed & explicit consent. In contrast, the US takes a more institutional or sector-specific approach that favours operational flexibility. While India's DPDP Act has built-in promising protections, further elaboration — more so for various emerging technologies including AI — is required. It inevitably means a radical reform of consent frameworks as we move towards a new age of AI-driven healthcare, linking an ongoing relationship with data, explainability, & individual rights. Establishing a globally consistent basis of consent — at least for the sharing of data across borders — will also be essential to the ethical, legal & equitable use of health data.

CYBERSECURITY MEASURES: A GLOBAL COMPARASION

Artificial Intelligence (AI) is moving its way into the realm of healthcare & while it provides phenomenal clinical capabilities, it also carries a complex set of cybersecurity risks. Healthcare

AI systems manage substantial quantities of sensitive personal information, including EHRs, genomic data, and real-time physiological monitoring., which makes them a target for cybercriminals. When these systems are breached, the safety, privacy & credibility of the institution are in question. As a result, national cyber security frameworks have emerged as integral components of data protection regimes. This section looks into the cybersecurity measures relied on in the EU, US & India and compares them in terms of health data observance in AI domains.

European Union: Integrated & Risk-Based Security Governance

There is a huge overlap between how the EU regulates both cybersecurity & privacy, essentially through the GDPR & the NIS Directive.

- **GDPR Security Obligations:** Article 32 of the GDPR requires that data controllers and processors implement "suitable technical and organizational measures" to ensure a level of security that matches the risk. These measures could encompass:
  - Implementation of pseudonymisation and encryption of private information;
  - Protecting the confidentiality, integrity, availability & resilience of processing systems;
  - Routine examination and assessment of protection systems.

The GDPR is risk-based, which means that security measures need be proportionate with (the data sensitivity & potential damage if a breach occurs (in terms of loss of the protection, trustworthiness, and accessibility of information). For AI systems, this signifies that developers & healthcare providers need to assess the risks that both automated processing & large-scale storage of data presents.

- **NIS Directive & NIS2:** To help enhance cybersecurity in key sectors, including healthcare, the NIS Directive (2016/1148) & the NIS2 Directive, which was adopted recently, bolster this area even further. These laws mandate that operators of essential services (OES) and digital service providers (DSP) must report cybersecurity incidents and implement cyber risk management practices. NIS2 broadens the scope of “essential entities” that healthcare providers using AI systems fall under, including maintaining strong incident response capabilities, business continuity planning, & technical security standards.

United States: Sector-Specific Cybersecurity Enforcement

In the U.S., the main source of cybersecurity in healthcare comes from the HIPAA & is

enforced by the dept. of HHS via its OCR.

- ***"HIPAA Security Rule"*:** It includes national standards to safeguard ePHI, with the HIPAA Security Rule. Key elements include:
  - Administrative safeguards — risk analysis, employee training, & security policies;
  - Technical safeguards: Data encryption and authentication; and
  - Technical controls: Access controls, audit controls, & data encryption.

Unlike the GDPR, HIPAA does not require encryption but instead deems it an "addressable implementation specification," meaning that entities need to have a reason if they do not implement it. Any AI that interacts with HIPAA-covered entities (e.g., hospitals, insurers) must adhere to these safeguards, but AI developers who aren't actively engaging covered entities may escape HIPAA's grasp, leaving cybersecurity governance gaps.

- **HITECH Act and OCR Enforcement:** In 2009, the HITECH Act promoted an explosion of digitising healthcare & tightened breach notification requirement. HITECH mandates that covered entities inform impacted individuals, HHS, and, in certain situations, the media about breaches involving 500 or more individuals. The OCR compels compliance through audits & has imposed heavy fines against institutions that do not establish appropriate safeguards. But with the absence of a national cybersecurity law on these unique AI risks, the United States has had to rely on sectoral & state-level action. They may also voluntarily comply with the NIST Cybersecurity Framework.[20]

India: A Patchwork in Transition

Cybersecurity in healthcare is an evolving area for India driven by inter alia the IT Act the DPDP Act, as well as guidelines specific to the healthcare sector.

- ***"The Information Technology Act & CERT-In"*:** Section 43A of the IT Act applies to companies that manage sensitive personal information responsible for data breaches caused by negligence. Although the *"Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal Data or Information) Rules, 2011"* require, to some extent, entities to adopt comprehensive security measures, the details on how that should be carried out are very vague. The CERT-In, an agency under the MeitY, is tasked with coordination of response activities to cyber incidents & distributing advisories. From April

[20] National Institute of Standards & Technology, Framework for Improving Critical Infrastructure Cybersecurity (2018).

2022, CEIR-In has made it mandatory that cyber incidents must be reported in six hours, which is quite a compliance burden for AI developers & hospitals.

- ***"Digital Personal Data Protection Act 2023"*:** While most of the provisions of the Act focuses on privacy, some sections mandate the Data Fiduciaries to adopt "reasonable security safeguards" in order to safeguard personal information. The Act mandates the secure notification of personal data breaches to both the Data Protection Board of India (DPBI) and the individuals impacted. But it lacks any mention of minimum-security standards or acknowledging AI-specific cybersecurity risks. Because there are no robust health-specific or AI-specific cybersecurity laws, legal uncertainty exists for those that use AI in the medical field. The Health Data Management Policy, released by India's National Digital Health Mission (NDHM), recommends that data be encrypted & minimised, but it remains just that, a policy document with no legal weight.[21]

Comparative Analysis

ASPECT	EU (GDPR/NIS)	US (HIPAA/HITECH)	INDIA (IT ACT/DPDP ACT)
ENCRYPTION REQUIREMENT	Recommended under GDPR, sectorally mandated in NIS2	Addressable (not mandatory) under HIPAA	Mandated indirectly under IT Rules, vague in DPDP Act
BREACH NOTIFICATION	Mandatory within 72 hours (GDPR)	Mandatory within 60 days (HITECH)	Mandatory within 6 hours (CERT-In), unspecified in DPDP Act
AI-SPECIFIC SECURITY LAW	Addressed in AI Act (proposed)	None at federal level	No AI-specific law, under development

[21] National Health Authority, Health Data Management Policy, Ayushman Bharat Digital Mission (2020).

INCIDENT RESPONSE OBLIGATIONS	Robust (NIS2 Directive)	Required under HIPAA, enhanced by NIST	Required by CERT-In guidelines

The level of readiness for cybersecurity differs across various jurisdictions. The EU sets leading travaux on a mandatory basis while the USA mixes optional plus obligatory arrangements. India's cyber governance framework is fragmented and more policy-driven than implementation-focused & lacks enforceable AI-specific norms. Cybersecurity is a vital pillar of AI governance in healthcare. The EU's strong, risk-based framework provides an overall holistic model for both data protection and cyber resilience. A sectoral approach with an emphasis on enforcement & industry standards characterizes the US approach. Although India is moving forward, it has to further set out statutory duties & AI-specific protections. In an age of cyber threats that are getting ever more sophisticated & globalized, cross-border harmonisation of the cybersecurity standards applied to AI systems that handle health data is crucial. Building a secure digital health infrastructure requires forward-looking legal infrastructures, ongoing risk assessment & adaptive governance.

LEGAL OBLIGATIONS AFTER DATA BREACHES

In recent years, numerous high-profile cyberattacks at leading hospitals have underscored that data breaches can threaten the functionality of AI, & in the realm of healthcare powered by AI systems, breaches are uniquely harmful to patient safety, privacy, & trust. A breach of sensitive health data can be catastrophic, leading to identity theft, medical fraud, reputational damage and legal liability. As artificial intelligence takes on a more significant role in processing health data—from diagnostic algorithms that conduct radiologic studies or pathology slides to predictive analytics that guide clinical or surgical decision-making—the risk of breaches have increased in both scope & complexity. Therefore, the duties towards respecting these breaches have been more so the focal point of data security legislation. The present section compares the legal requirement for breach notification and post-breach response in the EU, US & India.

European Union: Stringent Obligations Under GDPR

The foundational cornerstone of the GDPR is strong & enforceable provisions regarding breach notification and response.

- **Advise to Supervisory Authorities:** Under Article 33 of the GDPR, data controllers are required to inform the appropriate supervisory authority within 72 hours after they become aware of a personal data breach, unless it is determined that the breach is unlikely to pose a risk to the rights and freedoms of individuals. The notification should contain:
  - The characteristics and extent of the violation;
  - Types and estimated number of individuals affected;
  - Potential impacts of the violation;
  - Measures implemented or suggested to address the violation

If you fail to notify, within the said timeframe, significant administrative fines in accordance with Article 83 may apply.

- **Notify to data subjects:** Article 34 requires controllers to alert individuals who are likely to be adversely impacted by the breach without delay. The notification must be expressed in clear, easy-to-understand language & include recommendations on how the individual can reduce harm. If the data is rendered unintelligible (e.g., by way of encryption), or if further action can measure should be implemented to reduce the risks faced by data subjects, then an exemption is provided. The GDPR therefore fosters transparency, accountability & remediation in that individuals will not be left in the dark when there is a breach of their data security.

United States: Sector-Specific Breach Notification Laws

There is no general federal breach notification law that applies to all covered entities in the US. Rather, breach response is regulated by a patchwork of federal & state laws, with healthcare data breaches mainly covered under the HIPAA & the HITECH Act.

- **Breach notification rule under HIPAA and HITECH:** The HIPAA Breach Notification Rule mandates that covered entities must inform:[22]Inform affected individuals without unreasonable delay and within 60 days of being discovered;
- Notify the Department of HHS if the breach impacts 500 or more individuals;
- Inform prominent media outlets if the breach affects more than 500 residents within a single state.
- Data that is protected by encryption is usually exempt from breach notifications unless that encryption has been compromised.

The notification must include a description of the breach along with the types of information

[22] 45 CFR §§ 164.400–414

involved, as well as steps individuals should take in response and the actions taken to reduce harm.

Laws mandating notification at the state level: Forty- Five states, along with the District of Columbia, Guam, and the Virgin Islands, have enacted their own legislation regarding data breach notifications, which often have broader definitions of personal data & shorter time frames for notifying victims. *"California's Consumer Privacy Act (CCPA)"*, for example, obligates businesses to inform impacted residents "in the most expedient time possible." US law is also quite fragmented, creating compliance challenges, including for multinational health care organizations & AI vendors that may also be active in multiple states.

India: Evolving Framework Under CERT-In & DPDP Act

India's obligations following a data breach are defined by our IT laws, the directions issued by CERT-In, & the newly launched DPDP Act.

- **CERT-In Guidelines:**[23] CERT-In, which functions as the component of the Ministry of Electronics & Information Technology (MeitY) dealing with cybersecurity, is at the helm of cybersecurity in India. In April 2022, CERT-In had introduced a new rule making it mandatory to report all security incidents, such as data breaches, within six hours of their detection. This goes for all the companies involved in sensitive personal data, including hospitals, insurance companies, & health-tech platforms. The report must include:
  - Details of the incident and its effects;
  - Impacted Systems & Services;
  - Actions: Mitigation and containment

Although useful for visibility into incidents, the six-hour rule has received some criticism for being operationally burdensome, particularly for smaller health organisations & AI developers.[24]\

- **DPDP Act Obligations:** The DPDP Act also establishes a more privacy-centric framework for loss notification. Data Fiduciaries are required to:
  - If there is an event of a personal data breach, notify the DPBI.;
  - Notify the impacted Data Principal (person) where the violation poses a danger of damage.

[23] CERT-In, Directions on Information Security Practices (April 2022).
[24] Rahul Matthan, 'The Challenges of CERT-In's Six-Hour Breach Reporting Mandate' (2022) The Economic Times.

- No time period is specified in the Act itself, & so it is to be prescribed by subsequent rules. It also fails to explain what "harm" means, which could result in under-reporting.

In addition, enforcement mechanisms under the DPDP Act are still in their infancy. The DPBI is not yet operationalised, & its powers & procedure are still being finalised. In theory, this makes India's post-breach response framework promising.

Comparative Overview

ASPECT	EU (GDPR)	US (HIPAA/STATE LAW)	INDIA (CERT-IN/DPDP ACT)
Supervisory Notification	Within 72 hours	Within 60 days (HIPAA)	Within 6 hours (CERT-In); TBD (DPDP)
Notification To Individuals	Mandatory for high-risk breaches	Mandatory for most breaches	Mandatory if harm is likely
Encryption Exemption	Yes	Yes	Not clearly specified
Enforcement Authority	Data Protection Authorities	HHS/OCR & State AGs	DPBI (proposed) & CERT-In
AI-Specific Guidance	Indirectly via GDPR/AI Act	Not directly addressed	Not yet specified

Each jurisdiction has a variation model for breach management. The EU's approach puts speed, clarity, & personal rights first, in contrast to layered, state-based systems in the US. Sectoral urgency for India (CERT-In) meets emerging privacy obligations (DPDP Act) — albeit with full implementation of itself pending. The impact of data breaches in AI-powered healthcare ecosystems is profound & multifaceted. Not only does any legal framework need to require expedient breach notification, but enforcement against organisations needs to be possible to be able to hold those affected to accounts. The EU model is considered the most rigid & clear-cut, while the US offers some flexibility through sector specific laws & India is on a transition towards a legal framework. As AI technologies use transnational pathways,

aligning breach response obligations will be critical towards ensuring public trust & supporting ethical advancement in the use of digital health technologies.

PATIENT TRUST: CULTURAL & LEGAL PERSPECTIVES

AI will be a part of the future; as a part of a healthcare system, it promises improved diagnostics, personalised therapy, efficiency of healthcare systems, & integrated technology. However, the successful implementation of AI in healthcare relies on one fundamental aspect: The trust of the patients. Trust plays a role in a patient's decision to share personal health data, act on AI-generated recommendations & interact with digital health platforms. It is moulded not merely by legal protections & institutional constraints but also by the historical experience with medical systems, deep-set cultural values and social norms. This section specifically investigates the construction & maintenance of trust in healthcare data systems — & in particular those underpinned by AI — across different jurisdictions, with the EU, US, and India as our focal points.

- **Defining Patient Trust in the AI Age:** The trust patients have there is multi-faceted:
  - Trust: Trust in the competence & integrity of healthcare institutions & AI developers.
  - Interpersonal trust: Trust in health care professionals to act in the patient's interest.
  - Technological trust: Trustworthiness of AI systems for targeting, biasness & discrimination.

These dimensions are intertwined with the external regulatory environment & cultural norms that can influence patient behaviours & expectations. It's not just sophistication of technology that's needed to maintain trust in AI-driven healthcare, where decisions may be made or aided by algorithms that aren't visible to the naked eye; we need transparency, accountability, ethical integrity, & legal guarantees in governance, to quote George W. Bush, that people can '…run & hide, but not from law'.[25]

- **European Union: A Rights-Based, Accountability-Driven Model:** The EU's approach to building trust in its healthcare data systems is grounded in a rights-based legal framework, especially the *GDPR (European Parliament & Council, 2016)*. GDPR includes principles like lawfulness, fairness, transparency, data minimisation, & purpose limitation to ensure that patients have assurance that their private health information is being managed ethically and securely. Furthermore, enforcement mechanisms under

[25] Luciano Floridi & Mariarosaria Taddeo, 'What Is Data Ethics?' (2016) 374 Philosophical Transactions of the Royal Society A 20160360.

GDPR—like data protection authorities & the right to complain or seek compensation—help keep institutions accountable, another pillar of trust. In the context of AI-driven healthcare, Article 22 of the GDPR, which ensures safeguards to decision-making based solely on automated processing, is especially significant. Beyond legal protections, attitudes in many EU countries are culturally disposed to intensive privacy protections. Surveys have repeatedly shown that compared to their counterparts in America or India, EU citizens are more likely to consider data privacy as a basic human right. This cultural orientation promotes tougher laws & creates public confidence in health systems that play by these rules. Indeed, & the proposed Artificial Intelligence Act — with its transparency & risk management requirements for high-risk AI systems — is a continuation of this trust based regulatory ethos.

- **United States: Institutional Trust & Consumer-Centric Frameworks:** In the US, patient trust is more closely associated with institutional reputation & technological innovation than with rights-based legal protections. The Health Insurance Portability & Accountability Act of 1996 (HIPAA), for example, provides at least a basic framework for privacy and security of health data (i.e., it places restrictions on how patient data can be used & shared by covered entities) but is often criticized for its limited scope (e.g., digital health applications, artificial intelligence systems, etc.) & its relevance to traditional health-care settings. Legal loopholes notwithstanding, US healthcare AI trust is largely based on brand trustworthiness, clinical validation, & market performance. Celebrities might even trust an AI-driven diagnostic app produced by a world-renowned academic hospital or tech firm, regardless of thorough legal oversight not being in place. American culture is inclined toward individual responsibility & technological optimism, often valuing convenience & access above privacy considerations. Consequently, countless users freely donate health data to apps or other platforms with little comprehension of data practices. But high-profile hacks & biased algorithms are slowly chipping away at this trust. The growing demand for algorithmic accountability — through measures such as the proposed Algorithmic Accountability Act — reflects an increasing recognition by the public & legislators of the need to strengthen legal protections to ensure patients can trust those with whom they interact & what they encounter when they access care.[26]
- **India: Trust Amidst Rapid Digitisation & Legal Transition:** Trust landscape in India is multi-faceted, influenced by cultural norms, health literacy & legal trajectories. In India,

[26] Daniel Solove, 'Privacy Self-Management & the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

patient trust has traditionally been based on personal relationships with healthcare providers, especially in rural or traditional settings. As digital health initiatives gain momentum, such as the Ayushman Bharat Digital Mission (ABDM), the dynamics of trust are evolving towards systems-level confidence in digital infrastructure. The DPDP Act contains critical guardrails, such as informed consent, notification of data breaches, & redress. In its current form, however, the Act lacks specificity regarding AI transparency, bias mitigation or even automated decision-making — all key to ensuring that patients retain trust in AI systems. Moreover, access to digital & health literacy is far from uniform across India, shaping how people view & engage with AI-powered healthcare. Perhaps not regulatory failure that undermines trust, but insufficient communication: a lack of user awareness. There are also cultural expectations. Trust in government-backed health schemes is sometimes stronger than in private actors in some communities. So, government endorsement or regulation of AI health tools can have a major impact on public trust.[27]

(i) Comparative Reflections:

DIMENSION	EU	US	INDIA
LEGAL FOUNDATION OF TRUST	Rights-based (GDPR, AI Act)	Sectoral & institutional (HIPAA)	Emerging (DPDP Act, policy frameworks)
DOMINANT TRUST MECHANISM	Legal accountability	Institutional reputation	Interpersonal & governmental
AI-SPECIFIC PROTECTIONS	Strong (Article 22, AI Act)	Weak or indirect	Minimal (in current legislation)
CULTURAL ORIENTATION	Privacy as a right	Innovation & convenience	Community-centric, diverse literacy

These differences imply that trust cannot be universalised but should be cultivated uniquely & contextually in a way that resonates with local legal regimes, facing challenges & working, facing & working with the initial & institutional culture. Trust is not (only) a by-product of regulation; trust is a prerequisite for the ethical and efficient use of AI in the healthcare sector.

[27] Parminder Jeet Singh, 'Data Sovereignty & Trust in India's Digital Ecosystem' (2022) IT for Change.

The presence of legal rights & institutional protections in the EU creates a high-trust space. Trust in the US is based on reputational & consumer-based factors, whereas in India it does not seem to have solidified yet & continues to be fluid & condition-based on both social norms & emerging legal structures. With AI systems becoming increasingly autonomous & complex, ensuring trust will require a multi-faceted approach—one that integrates sound legal frameworks, clear technology design & communication strategies sensitive to cultural differences. Without trust, even the best AI tools will be unable to fulfil their promise in healthcare.