Volume 3, Issue 4 ISSN 2582-743X

A Comparative Analysis of AI-Driven Healthcare Data Protection: Assessing India's Legal and Ethical Frameworks against the USA, EU, and Australia

Laxmi
Research Scholar,
Mody University School of Science and Technology,
Lakshmangarh, Sikar, Rajasthan

****Dr. Pooja Jain***
Assistant Professor,
School of Law, Mody University of Science and Technology,
Lakshmangarh, Sikar, Rajasthan

ABSTRACT

The integration of Artificial Intelligence (AI) into healthcare systems has revolutionised medical diagnostics, patient management, and treatment methodologies. However, this advancement comes with significant concerns about data protection, privacy, and ethical governance, particularly in countries with diverse legal frameworks. This research provides a comparative analysis of AI-driven healthcare data protection in India, the USA, the EU, and Australia. It critically examines the effectiveness of India's legal and ethical frameworks, such as the Digital Personal Data Protection Act (DPDPA) 2023, the proposed Digital Information Security in Healthcare Act (DISHA), and existing regulations, against well-established global counterparts, including the EU's General Data Protection Regulation (GDPR), the USA's Health Insurance Portability and Accountability Act (HIPAA), and Australia's Privacy Act 1988. The paper explores enforcement mechanisms, patient rights, regulatory compliance, and challenges unique to each jurisdiction. Finally, it provides recommendations for strengthening India's data protection regime by adopting global best practices while ensuring AI-driven healthcare innovation remains ethical and legally sound.

Keywords: *Artificial Intelligence, Healthcare Data Protection, Privacy, Legal Frameworks, India, USA, EU, Australia, AI Ethics, Regulatory Compliance.*

INTRODUCTION

Precision medicine, predictive analytics, and automated diagnostics are made possible by AI, which is transforming the global healthcare industry and enhancing patient outcomes and healthcare efficiency (He et al., 2019). AI-powered healthcare systems handle enormous volumes of private health information from wearable technology, genetic sequencing, Electronic Health Records (EHRs), and real-time patient monitoring systems (Jiang et al., 2017). Despite the enormous promise of AI applications in healthcare, there are serious issues with data privacy, security, algorithmic transparency, and ethical governance (Leslie, 2019). Strong legal and ethical frameworks are required in order to control AI-driven healthcare and guarantee the security of patients' private medical data.

Volume 3, Issue 4 ISSN 2582-743X

Different legal traditions, policy agendas, and technical governance methods are reflected in the many regulatory systems that different nations have created to secure healthcare data powered by AI. According to Voigt and Bussche (2017), GDPR of the EU has created one of the strictest regulatory frameworks. It requires clear patient permission, data minimization, accountability procedures, and severe penalties for non-compliance. In contrast, the US mainly uses the Health Insurance Portability and Accountability Act (HIPAA) to control the security and privacy of healthcare data; nevertheless, HIPAA does not particularly address algorithmic accountability or AI-driven decision-making (McGraw, 2019). The My Health Records Act of 2012 and the Privacy Act of 1988 oversee Australia's data protection laws, which are now undergoing revisions to improve data security and AI governance (Greenleaf, 2020). In contrast, the Digital Personal Data Protection Act (DPDPA) 2023, which was recently passed in India, establishes the framework for data protection in the digital era but excludes measures pertaining to AI (Matthan, 2023). According to Singh et al. (2022), there is also ambiguity around India's healthcare AI regulations since the planned Digital Information Security in Healthcare Act (DISHA) seeks to control digital health data but has not yet received legislative approval.

A number of data privacy issues arise from the growing use of AI in healthcare. Large datasets, sometimes including sensitive medical records and personally identifiable information (PII), are necessary for AI models to be trained and to increase their forecast accuracy (Mittelstadt, 2019). Regulators place a high premium on data security and privacy protections because unauthorized access, cyberattacks, and data breaches represent serious threats to patient confidentiality (Goodman & Flaxman, 2017). AI algorithms may also be biased and opaque, which might result in prejudice when making healthcare decisions (Floridi et al., 2018). Biased training data, for example, may lead to incorrect diagnoses or disproportionate treatment recommendations for patients from underrepresented groups in AI-driven diagnostic systems (Topol, 2019). Furthermore, the absence of explicit accountability procedures raises questions about responsibility in situations when AI-driven choices result in ethical transgressions or medical blunders (Kaminski, 2020). Given these dangers, a clear legal and ethical framework is necessary to control AI's use in healthcare and guarantee adherence to international norms.

Several essential components should be included in a successful legislative framework for the security of AI-driven healthcare data. According to Schwartz and Solove (2014), strict security protocols, permission requirements, and anonymization strategies should all be used to secure patient data. AI-driven medical decision-making should be transparent, equitable, and explicable, according to ethical AI governance (Moor, 2018). Policies for global data sharing while upholding strict privacy standards should be outlined in cross-border data transfer rules (Leslie, 2019). Finally, accountability and enforcement systems need to enable regulatory bodies to keep an eye on AI-powered medical applications and punish non-adherence (McGraw, 2019). Although HIPAA mainly addresses data security in the healthcare sector, it does not address AI bias and transparency (Voigt & Bussche, 2017). In contrast, the GDPR provides a complete model with stringent enforcement requirements and explicit patient rights. Although Australia's legal system is changing, there are still holes in its AI governance.

Volume 3, Issue 4 ISSN 2582-743X

Although DISHA and India's DPDPA 2023 provide fundamental rules, further work is required to properly handle dangers unique to AI (Matthan, 2023).

In light of the fragmented global regulatory environment, the purpose of this research study is to compare the legislative frameworks for AI-driven healthcare data protection in the US, Australia, the EU, and India. The research aims to address many important concerns, such as: (1) How are AI-driven healthcare data protection regulations in various jurisdictions? (2) What are the advantages and disadvantages of every framework? and (3) How can India use best practices from across the world to enhance its regulatory approach? Through this comparative analysis, the study will provide light on how India may create a strong ethical and legal framework that guarantees AI-driven healthcare innovation stays transparent, patient-centered, and consistent with the law (Singh et al., 2022).

This paper has the following structure: The legal and ethical frameworks controlling the security of AI-driven healthcare data in Australia, the US, the EU, and India are thoroughly reviewed in Chapter 2. A comparative examination of enforcement procedures, strengths, and shortcomings across jurisdictions is presented in Chapter 3. Key legal issues and shortcomings in India's present regulatory framework are identified in Chapter 4. Policy suggestions are provided in Chapter 5 to improve India's strategy for protecting AI-driven medical data. The investigation is finally concluded in Chapter 6, which also offers a summary of the results and recommendations for further research.

Maintaining a balance between strong data security and technical innovation is essential as AI continues to influence the healthcare industry. By examining worldwide best practices and legal issues, this study adds to the current policy debates on how India might improve its regulatory environment to establish a safe, moral, and AI-ready healthcare system that complies with international data protection policies.

LEGAL AND ETHICAL FRAMEWORKS IN AI-DRIVEN HEALTHCARE

Medical diagnosis, treatment approaches, and individualized care have all been transformed by the quick adoption of AI in healthcare. However, there are serious issues with algorithmic accountability, patient data privacy, ethical issues, and regulatory supervision brought up by the growing dependence on AI-driven decision-making (Leslie, 2019). Because AI in healthcare depends on large datasets, like as genetic data, behavioral health records, and sensitive personal health information (PHI), a thorough legal framework is required to guarantee data protection, patient permission, and ethical AI deployment (Tsamados et al., 2021). Different legal and ethical frameworks have been created by nations worldwide to control AI-driven healthcare systems, resulting in differing degrees of enforcement and protection.

The legal and ethical frameworks controlling the protection of AI-driven healthcare data in Australia, the US, the EU, and India are compared in this section. With an emphasis on data privacy regulations, AI ethical rules, and new policy trends, the conversation focuses on important regulatory tools, patient rights safeguards, AI accountability systems, and

Volume 3, Issue 4 ISSN 2582-743X

enforcement difficulties. This section looks at various frameworks to find gaps and best practices in AI healthcare governance. It also provides information on how India may improve its regulatory environment.

European Union (EU): General Data Protection Regulation (GDPR) and AI Act

The GDPR (Regulation (EU) 2016/679), which places strict restrictions on the gathering, handling, and archiving of personal health data, is regarded as the gold standard for data protection (Voigt & Bussche, 2017). GDPR is a worldwide standard for AI healthcare data governance as it applies to any organization handling the personal data of EU citizens (Tikkinen-Piri et al., 2018). Important Aspects of GDPR in AI-Powered Healthcare:

- *Data Protection Principles:* GDPR ensures AI-driven healthcare systems handle only essential and pertinent health data by enforcing data reduction, purpose restriction, transparency, and accountability (EDPB, 2020).
- *Explicit Patient Approval:* In accordance with Article 9, processing sensitive health data necessitates the express approval of the patient, unless there are exclusions for scientific study, public interest, or medical necessity (Wachter et al., 2017).
- *Automated Decision-Making and Right to Explanation:* According to Wachter et al. (2017), Article 22 guarantees human supervision for medical AI applications by limiting fully automated AI decision-making in healthcare.
- *Cross-Border Data Transfers:* GDPR places stringent requirements on the transmission of health data across borders, necessitating the implementation of Standard Contractual Clauses (SCCs) and other suitable protections (Kuner et al., 2020).

The proposed EU AI Act seeks to regulate high-risk AI applications in healthcare in addition to GDPR by enforcing algorithmic transparency standards, obligatory risk assessments, and bias mitigation measures (European Commission, 2021). The Act designates AI healthcare systems as high-risk, requiring ongoing monitoring, human supervision, and audits for regulatory compliance (Smuha, 2021).

The GDPR and AI Act provide compliance challenges despite their robust legislative protections, particularly for small-scale AI healthcare developers. Furthermore, in complicated AI-driven medical decision-making, enforcement is difficult due to the right to explanation's continued ambiguity (Morley et al., 2020).

United States (US): Health Insurance Portability and Accountability Act (HIPAA) and AI Policy Developments

The US has a fragmented sectoral approach to data protection, with HIPAA (1996) managing healthcare privacy, in contrast to the EU's comprehensive privacy legislation (McGraw, 2019). However, there are legal loopholes in AI-driven healthcare systems since HIPAA was not created for AI applications (Kaminski, 2020). HIPAA Features for AI-Powered Healthcare are as following:

Volume 3, Issue 4 ISSN 2582-743X

- *The Privacy Rule:* This law safeguards personally identifiable health information and governs the use of PHI by AI-powered healthcare providers (Office for Civil Rights, 2013).
- *Security Rule:* To protect health data from cyber risks and vulnerabilities associated to AI, this rule mandates administrative, technological, and physical measures (Gomez, 2021).
- Re-identification issues still exist even if de-identification standards let AI developers to handle anonymised medical data without HIPAA constraints (McGraw, 2019).

The White House AI Bill of Rights (2022) calls for AI applications in healthcare to be fair, transparent, and bias-free (White House, 2022). AI-powered diagnostic tools are governed by the FDA's AI/ML Software as a Medical Device (SaMD) Framework, which guarantees algorithmic efficacy and safety (FDA, 2021).

Because AI-driven healthcare apps are not explicitly regulated by HIPAA, governance varies across states and institutions. Particularly for AI-powered diagnostics and robotically aided operations, the absence of harmonized federal AI rules leads to regulatory ambiguity (Kaminski, 2020).

Australia: Privacy Act 1988 and My Health Records Act, 2012

There are issues with AI-driven healthcare governance since Australia's Privacy Act 1988 and My Health Records Act 2012, which regulate healthcare data privacy, do not specifically address AI (Greenleaf, 2020). Australia's AI Healthcare Regulations' salient features include:

- Establish data protection guidelines for the gathering, processing, and consent of health data under the Australian Privacy Principles (APPs) (OAIC, 2019).
- A nationwide framework for digital health records that enables AI-powered analytics while adhering to stringent patient control guidelines (Lupton, 2020).
- The Australian Government's 2019 AI Ethics Principles are a voluntary framework that encourages responsibility, equity, and openness in AI healthcare applications.

AI-specific legislation is still lacking, despite the fact that privacy laws provide certain safeguards. The influence of the voluntary AI ethical standards on actual AI deployments is limited since they are not legally enforceable (Greenleaf, 2020).

India: Digital Personal Data Protection Act (DPDPA) 2023 and Proposed DISHA Framework

With the planned Digital Information Security in Healthcare Act (DISHA) and the Digital Personal Data Protection Act (DPDPA) 2023 intended to regulate health data privacy, India's AI healthcare governance is still developing (Matthan, 2023). Important Aspects of India's AI Healthcare Laws are:

- DPDPA 2023 creates guidelines for protecting personal data and mandates that patients provide their express permission before any health data may be used (Matthan, 2023).

Volume 3, Issue 4 ISSN 2582-743X

- The proposed DISHA aims to guarantee patient autonomy and interoperability by introducing AI-specific healthcare data security regulations (Singh et al., 2022).
- India's AI strategy places a strong emphasis on the ethical use of AI, but it lacks effective enforcement measures (NITI Aayog, 2021).

With no specific AI healthcare governance legislation, India's AI healthcare regulations are still in their infancy. To solve issues with algorithmic accountability, AI bias, and cross-border data flow, the DPDPA and DISHA need to be significantly improved (Matthan, 2023).

Global AI-driven healthcare data protection policies include gaps and inconsistencies, according to the comparison study. The US is still divided, but the EU is leading with the GDPR and the AI Act. While India's legal system is still developing, Australia's voluntary AI ethical rules are not legally binding. To guarantee reliable AI-driven healthcare systems, future legislative advancements must address AI justice, transparency, patient rights, and algorithmic accountability.

COMPARATIVE ANALYSIS OF LEGAL AND ETHICAL FRAMEWORKS IN AI-DRIVEN HEALTHCARE

The following table provides in-depth analysis across key aspects such as data protection laws, AI governance, patient consent, accountability, transparency, bias mitigation, enforcement, and compliance burdens.

Aspect	European Union (EU)	United States (US)	Australia	India
Primary Data Protection Law	General Data Protection Regulation (GDPR) (2016) – Comprehensive data protection law requiring explicit consent, data minimization, right to erasure, and strict cross-border transfer rules (Voigt & Bussche, 2017).	Health Insurance Portability and Accountability Act (HIPAA) (1996) – Focuses on health data privacy and security but does not explicitly regulate AI-based decision-making (McGraw, 2019).	Privacy Act 1988 – Covers personal and health data, requiring organizations to follow Australian Privacy Principles (APPs) (Greenleaf, 2020).	Digital Personal Data Protection Act (DPDPA) 2023 – Establishes personal data protection rights but lacks detailed AI-specific provisions (Matthan, 2023).
AI-Specific Regulations	Proposed AI Act (2021) –	FDA AI/ML-Based Software	AI Ethics Principles	Proposed Digital

Volume 3, Issue 4 ISSN 2582-743X

	Introduces risk-based AI classification, compliance rules, and mandatory human oversight for high-risk AI applications in healthcare (European Commission, 2021).	as a Medical Device (SaMD) Framework – Regulates AI-powered healthcare applications, but broader AI governance remains fragmented (Kaminski, 2020).	(2019) – Outlines voluntary ethical AI guidelines emphasizing fairness, accountability, and transparency, but lacks legal enforcement (Australian Government, 2019).	Information Security in Healthcare Act (DISHA) – Aims to regulate AI-driven healthcare applications, but still pending legislative approval (Singh et al., 2022).
Consent Requirements for AI in Healthcare	Explicit and informed patient consent required before AI processes sensitive health data (GDPR, Art. 9) (Wachter et al., 2017).	HIPAA requires patient consent for health data sharing, but AI-specific informed consent rules are absent (McGraw, 2019).	My Health Record system follows opt-in consent, allowing patients to control their health data access (Greenleaf, 2020).	DPDPA mandates explicit consent, but lacks AI-specific informed consent provisions (Matthan, 2023).
AI Accountability and Human Oversight	Mandatory human oversight for high-risk AI systems, such as AI-driven medical diagnoses (European Commission, 2021).	FDA ensures oversight of AI-based medical devices, but broader AI accountability remains unregulated (Kaminski, 2020).	AI Ethics Principles encourage human oversight, but do not legally require it (Australian Government, 2019).	No AI accountability law yet; DISHA is expected to introduce AI governance rules (Singh et al., 2022).
Right to Explanation and AI Transparency	GDPR Article 22 guarantees the right to explanation when AI-driven healthcare	No federal right to explanation for AI decisions; some state laws promote AI transparency	AI transparency is encouraged, but not legally enforced (Greenleaf, 2020).	Lack of AI transparency laws; DPDPA does not mandate explainability

Volume 3, Issue 4 ISSN 2582-743X

	decisions impact patients (Wachter et al., 2017).	(McGraw, 2019).		(Matthan, 2023).
Bias and Algorithmic Fairness in AI	AI Act requires AI risk assessment, bias mitigation, and fairness audits (European Commission, 2021).	White House AI Bill of Rights (2022) promotes guidelines for AI fairness, but lacks legal enforcement (Kaminski, 2020).	Voluntary AI Ethics Principles emphasize fairness, but compliance is not mandatory (Australian Government, 2019).	No explicit provisions addressing AI bias; fairness principles are not covered in DPDPA or DISHA (Singh et al., 2022).
Cross-Border Data Transfers	Strict international data transfer restrictions under GDPR (Standard Contractual Clauses, adequacy requirements) (Kuner et al., 2020).	HIPAA does not restrict cross-border transfers, but some states impose additional regulations (McGraw, 2019).	Australian Privacy Principles (APPs) require offshore data compliance but do not prohibit transfers (Greenleaf, 2020).	DPDPA 2023 mandates government approval for cross-border health data transfers (Matthan, 2023).
Regulatory Enforcement and Penalties	European Data Protection Board (EDPB) can impose fines up to 4% of global turnover for AI-related privacy violations (European Commission, 2021).	Department of Health & Human Services (HHS) enforces HIPAA, but AI-specific enforcement remains weak (McGraw, 2019).	Office of the Australian Information Commissioner (OAIC) monitors privacy compliance, but AI enforcement is voluntary (Greenleaf, 2020).	Data Protection Board (DPB) under DPDPA will oversee AI governance, but details remain unclear (Matthan, 2023).
Compliance Burden on AI Healthcare Providers	High – Healthcare providers must meet GDPR and AI Act compliance	Moderate – HIPAA compliance is required, but AI-specific rules	Low – AI Ethics Principles are voluntary, reducing regulatory burdens	Evolving – DPDPA and DISHA regulations may increase compliance

Volume 3, Issue 4 ISSN 2582-743X

	requirements (Voigt & Bussche, 2017).	vary (Kaminski, 2020).	(Australian Government, 2019).	costs (Matthan, 2023).

Key Takeaways from the Comparative Analysis

- EU has the most comprehensive AI healthcare governance framework, ensuring strict patient protection, accountability, and transparency (European Commission, 2021).
- The US follows a fragmented approach, with HIPAA and FDA regulations covering health data and medical AI applications, but lacking federal AI-specific protections (McGraw, 2019).
- Australia prioritizes AI ethics over strict regulations, leading to self-regulation and voluntary compliance rather than mandatory legal oversight (Greenleaf, 2020).
- India is in the early stages of AI healthcare regulation, with DPDPA 2023 covering data protection and DISHA expected to introduce AI-specific healthcare governance (Matthan, 2023).
- EU and India impose strict cross-border data restrictions, while US and Australia allow more flexible data transfers (Kuner et al., 2020).
- AI accountability and bias mitigation are strongest in the EU, while the US and Australia rely on voluntary guidelines, and India has yet to introduce explicit rules (Singh et al., 2022).

The EU's stringent regulations provide the strongest data protection framework for AI-driven healthcare but result in higher compliance costs. The US allows more flexibility, encouraging AI innovation but lacking unified data governance standards. Australia promotes self-regulation with ethical AI guidelines rather than strict enforcement. India is still developing its AI healthcare regulatory landscape, and DISHA is expected to play a crucial role in addressing AI accountability and transparency in the future.

For India to ensure responsible AI healthcare governance, policymakers should incorporate AI accountability measures from the EU, establish AI fairness principles similar to Australia, and develop robust enforcement mechanisms to balance innovation with privacy protection.

RECOMMENDATIONS FOR STRENGTHENING INDIA'S FRAMEWORK

AI has become a transformative force in the healthcare industry, offering innovative solutions in medical diagnostics, treatment planning, and operational efficiency. However, as AI systems increasingly rely on vast amounts of patient data, significant privacy, ethical, and legal concerns arise. In India, the regulatory framework governing AI-driven healthcare remains fragmented and insufficiently developed compared to global standards. While countries such as US, EU, and Australia have established robust legal mechanisms to protect patient data and

Volume 3, Issue 4 ISSN 2582-743X

regulate AI applications in healthcare, India's framework is still evolving. The DPDPA, 2023, which aims to protect personal data, lacks specific provisions addressing AI-driven decision-making, algorithmic bias, and AI transparency (Matthan, 2023). Furthermore, the Digital Information Security in Healthcare Act (DISHA), which was proposed to regulate health data protection, has not yet been enacted, leaving a significant legal vacuum in AI healthcare governance (Singh et al., 2022).

The absence of a dedicated AI healthcare regulatory framework poses critical challenges, including risks associated with automated decision-making, inadequate patient consent mechanisms, and the potential for algorithmic bias in medical treatments. While the EU's GDPR, the US' Health Insurance Portability and Accountability Act (HIPAA), and Australia's Privacy Act have well-defined provisions addressing AI-driven healthcare applications, India's legal framework lacks clear guidelines on AI accountability, liability, and data-sharing policies (European Commission, 2021; McGraw, 2019). To align India's regulatory framework with global best practices, comprehensive legal and ethical reforms are necessary. This section provides detailed recommendations for strengthening India's AI healthcare framework, focusing on legislative reforms, AI transparency, bias mitigation strategies, ethical governance, and enhanced patient rights.

Legislative Reforms: Strengthening DPDPA and Enacting AI-Specific Healthcare Laws

One of the most pressing issues in India's AI healthcare governance is the absence of a dedicated legal framework that regulates AI-driven medical applications. The DPDPA 2023, while offering general data protection guidelines, does not address AI-specific concerns such as automated decision-making, explainability, and algorithmic accountability (Matthan, 2023). To enhance legal clarity and safeguard patient rights, amendments to the DPDPA should be introduced to incorporate AI-specific provisions, including mandatory AI impact assessments (AIA) for healthcare applications, a risk-based classification system for AI models similar to the EU AI Act, and clear guidelines on AI-driven medical data processing (Kuner et al., 2020). These legal amendments should ensure that AI systems deployed in healthcare maintain high standards of fairness, accuracy, and accountability.

Furthermore, the lack of a sector-specific AI healthcare law leaves hospitals, digital health startups, and AI developers in a regulatory gray area. In contrast, the United States' HIPAA mandates strict provisions on the processing and sharing of health-related data (McGraw, 2019). To bridge this gap, India should introduce a National AI Healthcare Regulation Act (NAIHRA), which explicitly governs AI applications in robotic surgery, predictive diagnostics, and clinical decision-making. Additionally, an independent AI regulatory authority should be established to oversee compliance with AI transparency and safety standards. This body should work closely with public and private healthcare stakeholders to create a balanced regulatory framework that encourages innovation while protecting patient privacy and rights.

Volume 3, Issue 4 ISSN 2582-743X

AI Transparency, Explainability, and Bias Mitigation Strategies

A critical concern in AI-driven healthcare is the lack of transparency and explainability in AI decision-making processes. Unlike the EU's GDPR, which grants individuals a "right to explanation" regarding AI-generated decisions, India's legal framework does not mandate AI transparency in healthcare applications (Kaminski, 2020). To ensure greater trust and accountability, India should introduce explainability requirements that compel healthcare institutions to disclose how AI-driven diagnoses and treatment recommendations are made. Additionally, AI audit trails should be implemented to provide a comprehensive record of AI decision-making processes, ensuring that healthcare providers and patients can understand and challenge AI-generated outcomes if necessary.

Bias in AI medical algorithms is another significant challenge. Studies have demonstrated that AI models trained on non-representative datasets can reinforce existing healthcare disparities, disproportionately affecting marginalized communities (McGraw, 2019). To mitigate this, regulatory measures should require demographic diversity in AI training datasets to ensure that AI-driven healthcare applications provide fair and unbiased medical recommendations. Furthermore, the adoption of fairness-aware machine learning (FAML) techniques should be encouraged to reduce algorithmic discrimination. Periodic AI bias audits should also be mandated to evaluate and rectify potential biases in AI-driven healthcare systems (Greenleaf, 2020).

AI Accountability, Liability, and Ethical Governance

The question of liability in AI-driven healthcare is another pressing concern that remains unaddressed in India's current legal framework. Unlike HIPAA in the US, which holds healthcare providers accountable for AI-induced errors, India lacks clear guidelines on AI liability and malpractice (Saxena et al., 2023). To establish legal accountability, India should introduce an AI legal liability framework, ensuring that responsibility for AI-driven medical errors is assigned appropriately to AI developers, healthcare providers, and AI system operators. Additionally, AI malpractice insurance should be mandated for hospitals deploying high-risk AI applications, providing financial safeguards for patients affected by AI-related medical errors.

Cross-Border Data Transfers and AI Compliance Standards

With the increasing globalization of AI-driven healthcare solutions, India must also refine its cross-border data transfer regulations. The DPDPA 2023 lacks explicit AI-specific policies on international healthcare data exchanges, creating uncertainty for global AI collaborations (Matthan, 2023). In contrast, the EU enforces Standard Contractual Clauses (SCCs) to regulate AI data transfers, ensuring that healthcare data shared across borders adheres to strict privacy standards (European Commission, 2021). India should adopt a similar approach by establishing AI-specific cross-border data transfer mechanisms, ensuring compliance with international privacy standards while enabling innovation in AI-driven healthcare solutions.

Volume 3, Issue 4 ISSN 2582-743X

Enhancing Patient Rights and AI-Informed Consent Mechanisms

Ensuring that patients have control over their data and understand how AI systems impact their medical decisions is essential for ethical AI deployment. Unlike GDPR, which enforces strict informed consent requirements, India lacks robust AI-informed consent mechanisms in healthcare (Kaminski, 2020). New regulations should mandate explicit opt-in requirements for AI data processing, ensuring that patients are fully aware of how AI systems are used in their treatment. Additionally, AI literacy programs should be developed to educate patients and healthcare professionals about the risks and benefits of AI-driven medical applications.

Developing a Robust AI Regulatory Framework

India must also establish a dedicated AI regulatory authority to oversee compliance with ethical AI deployment in healthcare. This body should create regulatory sandboxes, allowing healthcare institutions to test AI applications in controlled environments before full-scale deployment (European Commission, 2021). Furthermore, collaboration between government agencies, healthcare institutions, and AI developers should be encouraged to balance technological innovation with ethical AI governance.

Roadmap for Strengthening India's AI Healthcare Laws

India stands at a critical juncture in shaping the future of AI-driven healthcare. While DPDPA 2023 and DISHA offer foundational legal protections, they are insufficient in addressing AI-specific concerns related to transparency, accountability, and patient rights. In comparison, the EU, US, and Australia have established comprehensive AI governance frameworks that India can learn from. Strengthening India's legal and ethical framework for AI-driven healthcare requires introducing AI-specific healthcare laws, enhancing patient rights, enforcing AI accountability, and ensuring compliance with global data protection standards. By adopting these measures, India can foster responsible AI innovation while safeguarding patient privacy and ethical AI deployment in healthcare.

CONCLUSION & A WAY FORWARD

The integration of AI in healthcare has revolutionized patient care, medical diagnostics, and hospital management. However, AI-driven healthcare also presents significant data protection and ethical challenges, necessitating a robust legal and regulatory framework. This study provides a comparative analysis of India's AI healthcare data protection laws against those of US, EU, and Australia, highlighting critical gaps and offering recommendations to strengthen India's legal and ethical framework.

India's data protection regime is still evolving, with the DPDPA, 2023 providing a foundation for data privacy, but lacking AI-specific regulations for healthcare (Matthan, 2023). The proposed DISHA (Digital Information Security in Healthcare Act) aims to address digital health data security concerns, but its enforcement and coverage remain uncertain (Singh et al., 2022). In contrast, the EU's GDPR provides one of the strongest data protection regimes globally, ensuring rigorous patient data security, AI transparency, and algorithmic

Volume 3, Issue 4 ISSN 2582-743X

accountability (European Commission, 2021). The US follows a sectoral approach, with HIPAA (Health Insurance Portability and Accountability Act) covering health data privacy but lacking a comprehensive AI-specific framework (McGraw, 2019). Australia, on the other hand, has adopted a flexible AI ethics approach, focusing on voluntary compliance rather than strict enforcement (Greenleaf, 2020).

This comparative assessment highlights India's urgent need to enhance AI-specific healthcare governance by implementing comprehensive AI accountability laws, transparency requirements, and ethical AI deployment strategies. The findings emphasize several key areas where India can align its legal and ethical AI frameworks with global best practices to ensure responsible AI-driven healthcare innovation. Unlike the EU AI Act and GDPR, which provide detailed AI governance mechanisms, India's DPDPA 2023 lacks sector-specific provisions for AI-driven healthcare data processing (Matthan, 2023). While DISHA is expected to introduce health data-specific regulations, it remains a draft proposal with uncertain implementation timelines (Singh et al., 2022). The EU's GDPR mandates strong AI transparency, data minimization principles, and algorithmic explainability, ensuring that AI-driven healthcare decisions are interpretable and accountable (European Commission, 2021). India currently lacks mandatory AI transparency provisions, making AI-driven healthcare systems more prone to opacity and patient distrust (Kuner et al., 2020). Unlike the EU, which applies a unified AI governance framework, the US follows a sectoral approach, with HIPAA covering health data privacy but lacking a federal AI-specific law (McGraw, 2019). AI governance in the US is largely industry-led, with state-level regulations emerging (Kaminski, 2020). India's approach somewhat mirrors the US model, relying on broad data protection laws rather than dedicated AI healthcare regulations (Saxena et al., 2023).

Australia has developed an AI Ethics Framework, which encourages responsible AI use through voluntary guidelines, rather than enforceable regulations (Greenleaf, 2020). This approach allows AI innovation but provides weaker data protection and accountability measures compared to the EU. India, too, has adopted a more flexible approach but requires stronger enforcement mechanisms to ensure patient data protection in AI-driven healthcare (Singh et al., 2022).

The EU has strict data localization and cross-border transfer rules, ensuring that healthcare data is protected even when transferred outside the EU (European Commission, 2021). The US, in contrast, follows less restrictive transfer policies, enabling global AI-driven healthcare collaborations (McGraw, 2019). India's DPDPA 2023 introduces data localization requirements, but its AI-specific implications remain unclear (Matthan, 2023).

To ensure responsible AI adoption in healthcare while protecting patient data, India should implement the following policy reforms:

- Introduce a comprehensive AI healthcare law that establishes clear rules for AI-driven medical decision-making, algorithmic accountability, and patient consent frameworks (Singh et al., 2022). Adopt a risk-based AI classification system, similar to the EU AI

Volume 3, Issue 4 ISSN 2582-743X

Act, ensuring high-risk AI applications undergo strict compliance measures (European Commission, 2021).

- Implement a "right to explanation" for patients impacted by AI-driven medical decisions (Wachter et al., 2017). Require AI developers to disclose training data sources, bias mitigation strategies, and decision-making criteria (Kuner et al., 2020).
- Establish clear liability frameworks holding AI developers, healthcare providers, and algorithmic decision-makers accountable for AI-related harm (McGraw, 2019). Implement bias audits and fairness testing for AI-based medical diagnosis and treatment systems (Kaminski, 2020).
- Establish Standard Contractual Clauses (SCCs) for AI-driven healthcare collaborations, aligning with GDPR's international data-sharing best practices (European Commission, 2021). Develop bilateral AI healthcare agreements with global AI regulatory bodies to enable secure international medical AI research (Saxena et al., 2023).
- Create a National AI Ethics Board to oversee AI healthcare applications and monitor AI fairness (Greenleaf, 2020). Implement GDPR-style penalties for non-compliance with AI transparency and fairness principles (Kuner et al., 2020).
- As AI in healthcare continues to advance, future research should explore the role of blockchain technology in enhancing AI-driven healthcare data security (Singh et al., 2022), impact of AI regulation on patient outcomes and medical ethics (McGraw, 2019), comparative AI governance models between emerging economies and developed nations (Kaminski, 2020), and effectiveness of algorithmic impact assessments in mitigating AI biases in healthcare (Wachter et al., 2017).

REFERENCES

- Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., … & Clark, J. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. arXiv preprint arXiv:2004.07213.
- Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389-399.
- Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501-507.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. International Data Privacy Law, 7(2), 76-99.
- Matthan, R. (2023). The Digital Personal Data Protection Act 2023: A critical analysis. New Delhi: Vidhi Centre for Legal Policy.
- Ministry of Electronics and Information Technology (MeitY). (2023). The Digital Personal Data Protection Act, 2023. Government of India. https://www.meity.gov.in
- Indian Council of Medical Research (ICMR). (2021). Ethical guidelines for AI-based healthcare research in India. https://main.icmr.nic.in/

Volume 3, Issue 4 ISSN 2582-743X

- Singh, P., Saxena, A., & Sharma, N. (2022). Data protection challenges in AI-driven healthcare: India's legal landscape. Journal of Law and Technology, 18(3), 234-256.
- Bhandari, V., & Chugh, S. (2023). Health data governance in India: An evaluation of DISHA and DPDP Act. Indian Journal of Law and Technology, 19(2), 78-101.
- European Commission. (2021). The EU AI Act: Proposal for a regulation laying down harmonized rules on artificial intelligence. Brussels: European Union. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- Kuner, C., Bygrave, L. A., & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A commentary. International Data Privacy Law, 10(1), 1-20.
- Veale, M., & Binns, R. (2017). Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, 383-394.
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.
- European Data Protection Board (EDPB). (2021). Guidelines on AI and data protection under the GDPR. Brussels: EDPB.
- McGraw, D. (2019). Building a strong foundation for health AI governance in the United States. Health Affairs, 38(10), 1614-1620.
- Kaminski, M. E. (2020). The right to an explanation, explained. Berkeley Technology Law Journal, 34(1), 189-220.
- Department of Health and Human Services (HHS). (2022). HIPAA and AI in healthcare: Addressing emerging challenges. Washington, DC: HHS Office for Civil Rights.
- United States Congress. (2023). The Algorithmic Accountability Act: Regulating AI in healthcare and data privacy. Washington, DC. https://www.congress.gov/
- Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
- Greenleaf, G. (2020). Australia's AI ethics principles: A new soft law approach. Computer Law & Security Review, 37, 105437.
- Australian Government. (2021). AI Ethics Framework: Responsible AI adoption in healthcare. Canberra: Department of Industry, Science, Energy and Resources. https://www.industry.gov.au/
- Australian Human Rights Commission (AHRC). (2022). Human rights and AI in healthcare: Ensuring fairness and accountability. Sydney: AHRC.
- Australian Privacy Foundation. (2023). AI and health data privacy in Australia: Challenges and reforms. Canberra: Australian Privacy Foundation.
- Bennett Moses, L., & Chan, J. (2021). Regulating AI in healthcare: The Australian perspective. Journal of Law, Medicine & Ethics, 49(2), 275-290.