Invited Article

Access this article online

Quick Response Code:

Website: https://journals.lww.com/ijar

DOI: 10.4103/ijar.ijar_340_25

Safe and Trusted Artificial Intelligence: Privacy as the cornerstone for digital transformation in Traditional Medicine

Abhishek Singh[1,2], Antara Vats[2]

ABSTRACT:

India possesses one of the world's oldest and richest treasuries of health knowledge, collectively known as Ayush: Ayurveda, Yoga and Naturopathy, Unani, Siddha, Sowa-Rigpa, and Homeopathy. Drawing upon millennia of wisdom, these indigenous sciences stand as globally recognized, effective systems of healthcare that bridge the knowledge of ancient times with the necessities of modern well-being. The increasing integration of Artificial Intelligence (AI) in healthcare marks a pivotal turning point in India's quest to bridge this gap but building scalable AI solutions to achieve large-scale social impact significantly on vast amounts of structured datasets. These datasets, in part, are being generated by key government platforms that aim to revolutionize healthcare delivery, research and data-driven decision-making: Ayushman Bharat Digital Mission (ABDM), launched by the Ministry of Health and Family Welfare (MoHFW) in 2021 and platforms like the Ayush Grid and the Ayush Health Information Management System, launched by the Ministry of Ayush (MoA) in 2018 form the comprehensive information technology foundation for traditional medicine. However, as healthcare data contain sensitive personally identifiable information, informational privacy becomes the cornerstone of safe and trusted AI development. The Digital Personal Data Protection Act (DPDP Act), 2023, establishes India's personal data governance framework. This paper illustrates how the DPDP Act instills a privacy-by-design approach for India's digital health ecosystem, offering actionable recommendations for augmenting ecosystem-wide compliance and underscoring the imperative to integrate safe and trusted AI principles throughout the digital health innovation lifecycle.

Keywords:

Ayush health information management system, Ayurveda, Ayush Grid, Data governance, Digital personal data protection act, Privacy, Safe and Trusted Artificial Intelligence

INTRODUCTION

Digital transformation of ancient wisdom

Ayush represents India's collective of traditional healthcare systems: Ayurveda, Yoga and Naturopathy, Unani, Siddha, Sowa-Rigpa, and Homeopathy. The history of these systems in India is ancient and diverse. Ayurveda is the foremost, with roots in the Atharva Veda (c. 1200 BCE) and formalized in classical texts such as the Charaka Samhita and Sushruta Samhita. Yoga was formalized by Patanjali around 2500 years ago. Unani and Siddha also have deep traditional roots in the subcontinent. Postindependence, in 1995, the Department of Indian Systems of Medicine and Homeopathy (ISM&H) was established, later renamed the Department of Ayush in 2003, recognizing the value of these systems. This marked a pivotal moment that prompted the mainstreaming of these indigenous practices into the national healthcare structure, culminating in the establishment of the dedicated Ministry of Ayush (MoA) in 2014.

An Ayurvedic clinic today blends ancient wisdom with modern technology.

[1]Ministry of Electronics and Information Technology, Government of India, [2]IndiaAI Mission, New Delhi, India

Address for correspondence:
Mrs. Antara Vats, Consultant, IndiaAI Mission, Electronics Niketan Annexe, 6 CGO Complex, Lodhi Road, New Delhi - 110 003, India.
E-mail: antaravats@alumni.nls.ac.in

Received: 09-11-2025
Revised: 13-11-2025
Accepted: 14-11-2025
Published: 06-12-2025

How to cite this article: Singh A, Vats A. Safe and Trusted Artificial Intelligence: Privacy as the cornerstone for digital transformation in Traditional Medicine. Int J Ayurveda Res 2025;6:286-92.

Practitioners collect patient data and store it digitally, pulse diagnostic devices capture digital waveforms, and mobile applications suggest personalized wellness regimens through *Prakriti*-based analysis. Ayushman Bharat Digital Mission (ABDM) by the Ministry of Health and Family Welfare (MoHFW) in 2021,[1] the Ayush Grid and the Ayush Health Information Management System (AHIMS) by the MoA in 2018,[2] marked historic milestones to digitize health systems in India. With nearly 12,000 Ayush facilities using cloud-based management systems and more being added every week, Ayush Grid lays a comprehensive Information Technology (IT) foundation for Traditional Medicine (TM) and is therefore a key source of structured data for the sector in India.[2] Mobile health applications have crossed 600,000 downloads. During Coronavirus Disease-2019, these digital platforms demonstrated their effectiveness by enabling real-time coordination between thousands of Ayush volunteers and facilitating the collection of treatment data through crowd-sourcing methods that would not have been feasible using paper-based records.

Integration of emerging technologies, including Artificial Intelligence (AI), holds enormous potential for Ayush, enabling predictive diagnosis and personalized treatment and improving early health risk detection. Tools such as AI-based *Prakriti* analysis, digital pulse interpretation, and language models that decode classical Ayurvedic texts are already reshaping traditional practice.[3] The Government of India announced the IndiaAI Mission with a budget allocation of around ₹10,000 crore to support the development and deployment of AI applications in critical sectors, including Ayush, to boost efficiency and accessibility of such AI-based applications.[4] Structured around seven pillars, the Mission proposes a whole-of-government approach to democratize access to compute resources, datasets, skilling initiatives, AI applications, and financing capital, to ensure the benefits of AI technologies and services reach the last mile. In particular, through the Safe and Trusted AI pillar, the Mission ensures the responsible development, deployment, and adoption of AI by implementing responsible AI projects, developing indigenous tools and frameworks, self-assessment checklists for innovators, and other guidelines and governance frameworks.

As AI increasingly integrates into the healthcare sector, patient and physician trust is a necessity for realizing the technology's revolutionary potential. The inherent risks within healthcare amplify the need for this mandate for robust safety and governance. AI's clinical integrity is dependent on the data it utilizes; if the underlying data is incomplete, for example, contain biases such as systematic underrepresentation of certain demographic groups, the AI models can lead to inaccurate diagnoses, posing a direct threat to patient safety. Furthermore, when an AI-driven recommendation results in patient harm, there must be clear and established lines of accountability, whether the responsibility ultimately rests with the prescribing clinician, the operating hospital, or the AI developer. Establishing this trust and accountability fundamentally requires transparency, allowing for an understanding of how the AI arrives at its conclusions.

Given AI's reliance on personal information, informational privacy protection becomes one of the foundational cornerstone of its responsible development and deployment. As such, this paper will focus on the risk to informational privacy with the large-scale development and deployment of AI-based applications in the Ayush domain. AI algorithms demand vast quantities of highly sensitive data – including Electronic Health Records (EHRs), diagnostic images, and genomic profiles – to achieve clinical efficacy. For example, an Ayurvedic consultation extends well beyond the conventional medical scope, limited to a chief complaint and diagnosis. An Ayurvedic consultation captures an unusually broad and profoundly personal spectrum of information, documenting an individual's constitutional type (*Prakriti*), daily and seasonal routines (*Dinacharya* and *Ritucharya*), detailed dietary habits and mental health status, multi-generational family history, and even, in some contexts, aspects of spiritual well-being.[5] These data are uniquely valuable and immutable, making any breach a permanent and catastrophic event. A core challenge is that the practice of anonymizing or deidentifying patient data often proves insufficient. This highly sensitive personal information must be safeguarded in alignment with a citizen's fundamental Right to Privacy, as recognized by the Hon'ble Supreme Court of India in the landmark judgment of Justice K. S. Puttaswamy (Retd.) and Another v. Union of India.[6]

The Digital Personal Data Protection Act, 2023 (DPDP Act), is India's first comprehensive framework balancing individuals' rights to protect their data with the imperatives of technological innovation.[7] It places user control and transparency at the core of personal data processing, creating not just obligations for data fiduciaries (i.e., person/s that determine the purpose and means of processing of personal data) but rights for citizens – a partnership model for data governance that aligns naturally with the patient-centric philosophy of TM.

This paper demonstrates how privacy protection and digital innovation can and must coexist in India's Ayush ecosystem. The paper is structured to connect policy, practice, and future compliance. Section 2 examines the digital transformation of healthcare in India, highlighting the enormous potential of AI applications

in the Ayush sector and India's pragmatic approach to data and AI governance. Section 3 highlights how the DPDP Act is one of the cornerstones of Safe and Trusted AI, ensuring informational privacy while enabling a thriving digital health ecosystem. Section 4 concludes with ecosystem-level recommendations that promote a privacy-by-design approach across all actors in the Ayush ecosystem, underscoring the critical need to integrate responsible AI practices throughout the healthcare innovation lifecycle. The paper ultimately demonstrates that the DPDP Act forms the bedrock upon which sustainable and trustworthy AI innovation can flourish.

DIGITAL TRANSFORMATION OF HEALTHCARE AND EVOLVING GOVERNANCE PRACTICES IN INDIA

AI opportunity in traditional medicine

AI has enormous potential in healthcare. NITI Aayog's National Strategy for AI recognizes healthcare as one of the key sectors that can benefit most from AI in solving societal needs. Ayush stands at the center of this transformation[8] by dramatically enhancing diagnostic accuracy, accessibility, and evidence-based practice. AI algorithms can detect the early signs of disease progression by analyzing patient records and treatment histories made accessible by the ABDM and Ayush Grid. This enables practitioners to recommend proactive, preventive measures and holistic care, forging a strong link between ancient knowledge and modern healthcare practices. Specific AI applications could include *Prakriti* determination, analyzing thousands of pulse readings to assist in traditional constitutional assessments, and treatment prediction, using machine learning models to forecast treatment outcomes based on individual constitutional types and lifestyle factors.[9]

A crucial application of AI lies in the preservation and interpretation of ancient medical texts. Natural language processing and multilingual AI tools can translate and interpret ancient Ayurvedic manuscripts. These technologies standardize terminology, making Traditional Knowledge (TK) available in multiple Indian languages, thus significantly increasing accessibility for practitioners and researchers. By utilizing AI to analyze and organize classical literature, traditional insights are structured and linked with modern medical research, demonstrably strengthening the scientific foundation of Ayush practices.[10] These initiatives will make TM more data-driven, globally credible, and aligned with India's vision for inclusive and responsible healthcare innovation.

India's digital health architecture

India's AI opportunity in healthcare will be enabled by its existing digital infrastructure, which includes ABDM and the Ayush Grid. ABDM serves as a digital backbone of India's healthcare ecosystem, enabling core components such as Ayushman Bharat Health Account IDs (ABHA IDs), healthcare professional registries, and a federated Health Information Exchange to work in cohesion. Notably, the system is designed to be medical-system agnostic, an ABHA ID functions seamlessly across different healthcare practices, whether modern or Ayurvedic.[11] With appropriate consent, an individual's health records may be securely shared across systems.

Ayush Grid[12] is a digital health platform launched by the MoA, Government of India, in 2018 as a comprehensive IT backbone for the entire TM sector in India. The primary vision of the Grid is to transform the Ayush sector to provide efficient, holistic, affordable, and quality services to all citizens through a secure and interoperable digital ecosystem, aligning seamlessly with ABDM. The Grid is a comprehensive digital architecture operating across National, State, and Citizen access levels, designed to ensure seamless digital connectivity for all Ayush stakeholders and realize the full potential of these traditional systems. This umbrella platform integrates several key projects, including the Ayush Hospital Information Management System, which links all Ayush facilities and is ABHA-enabled for digitized patient records; the National Ayush Morbidity And Standardized Terminologies Electronic (NAMASTE) Portal, which standardizes vocabulary and monitors disease patterns; and Ayush Suraksha, a pharmacovigilance platform essential for documenting adverse drug reactions and monitoring drug safety across all Ayush streams. Projects such as the TK Digital Library are integrated to safeguard indigenous knowledge and provide a global model for preservation and responsible use of medical heritage.

The establishment of this comprehensive digital infrastructure enables the advancement of AI in traditional healthcare, yet this integration elevates AI risks, including informational privacy. The sheer scale and sensitive nature of the digital health data managed through the platforms make it highly susceptible to reidentification attacks. Furthermore, if training datasets lack diversity, the resulting AI can propagate algorithmic bias, leading to discriminatory care. Consequently, ensuring safe and trusted AI development and deployment becomes essential for sustainable and equitable growth.

India's AI governance approach

India's approach to AI governance supports a pro-innovation, responsible ecosystem embedding

practical safety measures in the innovation lifecycle. NITI Aayog, has identified principles for responsible AI which should guide the development and deployment of AI. These include the principles of safety and reliability, equality, inclusivity and nondiscrimination, privacy and security, transparency, accountability and protection, and reinforcement of positive human values.[13] Further, the IndiaAI Mission under the Safe and Trusted AI pillar has initiated several key projects with support from academia, industry, and research organizations to create the necessary technical guardrails, such as privacy-enhancing tools, explainable AI, and algorithm auditing tools, among others.[14] Moreover, India AI Governance Guidelines were announced recently to provide a framework for the development and deployment of trustworthy, safe, inclusive, accountable, and responsible AI models and applications. The guidelines lay down foundational principles such as accountability, fairness, inclusivity and safety to ensure that AI systems remain human-centric and trustworthy. It outlines actionable measures to aid enablement, regulation and oversight covering infrastructure, risk management and accountability.

Specifically, in the healthcare sector, the ABDM adopts a "privacy-by-design" approach, implemented through federated digital architecture and the Consent Manager (CM) framework. This ensures informational privacy while enabling a thriving innovation ecosystem with seamless data sharing among stakeholders.

Further, to ensure ethical conduct and address emerging ethical challenges of applying AI in biomedical research and healthcare, the Indian Council for Medical Research (ICMR) has released guidelines, which provide a framework for ethical decision-making during the development, deployment, and adoption of AI-based solutions.[15] The guidelines recognize the importance of privacy in the healthcare sector due to the sensitive nature of health data and recommend appropriate anonymization protocols before sharing patient data for AI development.

Given the pivotal role of digital health data in fostering a robust innovation ecosystem that addresses India's societal challenges and accelerates transformation in the healthcare sector, safeguarding information privacy is essential. The DPDP Act provides a comprehensive framework to address personal data protection risks across all sectors and technologies and is discussed in detail in the next section.

UNDERSTANDING THE DPDP ACT, 2023

The Government of India enacted the DPDP Act on August 11, 2023, to govern the collection and processing of digital personal data. It mandates organizations collecting and processing digital personal data to obtain explicit consent, which must be free, specific, informed, unconditional, and unambiguous.[16] In practice, this means no hidden terms buried in lengthy agreements and no pre-selected consent boxes. The law empowers individuals with meaningful control over their data. This means citizens can withdraw consent at any time, request corrections to inaccurate information, and demand deletion of their data where there is no legal basis to retain it. They may also appoint a "nominee" to exercise their rights in case of death or incapacitation.[17] The Act follows a privacy-by-design approach as the enforcement mechanism is digital-first. The Data Protection Board, once established, will have its key processes, such as consent management and grievance redressal, be obtained through digital applications.[18]

Organizations handling large volumes of sensitive personal data may be notified as "Significant Data Fiduciaries" and face stricter requirements like mandatory privacy impact assessments, annual audits, and appointment of data protection officers.[19] As per the Act, the outlined measures can be undertaken to ensure that personal data is processed in accordance are depicted in Table 1.

Safeguarding health data under the DPDP Act

For healthcare, the DPDP Act provides a comprehensive framework covering the entire digital personal data collection and processing lifecycle, including key entities such as hospitals, insurers, research institutions, and digital health platforms.[20]

The ABDM, through its privacy-by-design approach and focus on user consent, ensures compliance with the DPDP Act as depicted in Figure 1.[21] The ABDM's federated architecture ensures that there is no centralized repository of health data. ABDM has developed a digital system called Health Information Exchange and CM, which ensures that the identity of persons intending to share information is first verified, consent of the person/patient is taken, logged, and only after that, the health records are shared between Health Information Providers and Health Information Users.

In compliance with the DPDP Act, ABDM's Health Data Management Policy acts as a guidance document that sets out the guidelines for data privacy protection. The policy emphasizes providing the user notice and obtaining their specific and informed consent for data sharing.[22]

As a result, an Ayurvedic hospital or practitioner can register on the respective registries of the ABDM integrating with the CM following federated architecture principles.

Table 1: Key compliance requirements under the DPDP Act, 2023

Compliance category	Compliance requirements
Applicability assessment	Identify whether the platform acts as a data fiduciary (controls purpose and means of processing) or data processor (acts on behalf of a fiduciary)
	DPDP Act applies if the platform processes digital personal data – including patient records, vital signs, doctor notes, etc., that identify individuals – even if processing occurs outside India but services target Indian users
Data collection and consent	Provide notice and obtain consent before collecting any personal data from users
	Notices must specify what data are collected, for what purposes, retention period, and grievance mechanisms
	Display notices in English and local languages and ensure affirmative, free, and informed consent
	Allow for withdrawal of consent at any time
Lawful and legitimate processing	Rely on legitimate uses permitted under the Act (e.g., compliance with a legal mandate and medical emergency) only when clearly justifiable
	Maintain documentation demonstrating the lawful basis for each processing activity
Data minimization and anonymization	Collect only data required for the platform's functionality
	As a proactive measure, the use of anonymized health data for AI model training
	Apply rigorous anonymization methods (e.g., de-identification, masking, and aggregation) and assess reidentification risks before using datasets
Technical and organizational measures	Implement robust security safeguards – encryption, access controls, audit logs, and breach notification protocols
	Appoint a DPO if designated as a significant data fiduciary
Individual rights	Enable users (data principals) to
	Access their personal data processed by the platform
	Correct or update inaccurate data
	Request data deletion or grievance redressal
	Nominate another person to exercise rights on their behalf in case of death/ incapacity
Breach management	Notify both the Data Protection Board and affected users in case of a data breach
	Maintain a response plan to contain and investigate incidents with documented follow-up actions

DPO=Data Protection Officer, DPDP=Digital Personal Data Protection, AI=Artificial Intelligence

When patients see their Ayush records protected by the same standards as their conventional medical records, trust is strengthened and privacy is preserved, regardless of which medical system is being used.

MAKING IT REAL: PRACTICAL ECOSYSTEM-LEVEL RECOMMENDATIONS

A wide range of actors contribute across the lifecycle of any digital ecosystem. In the healthcare context, this includes healthcare providers, research institutions, technology and platform companies, policymakers, regulators, and end-users. Traditional governance models often fall short when they address these stakeholders in isolation. As a result, the India AI Governance Guidelines highlight the importance of adopting an ecosystem-wide approach, which enables more holistic and effective outcomes.[23] Such an approach also helps clarify the distribution of roles and responsibilities among the diverse actors involved, fostering greater accountability and coordination. The following ecosystem-level recommendations ensure that informational privacy is ensured across the entire AI innovation lifecycle.

Platform developers and tech companies

Privacy should be integrated into system design from the outset. Open standards such as Health Level Seven Fast Healthcare Interoperability Resources for health records and ISO terminologies for interoperability should be adopted.[24] ABDM-compliant consent management frameworks must be integrated at the initial stage. Further, regular security audits are essential. Platform developers and enterprises should engage accredited third-party assessors and work toward ISO 27001 certification. In an environment of frequent data breaches, platforms that can demonstrably protect user data will gain both trust and market share.

Ayush healthcare providers

Privacy begins with people. All healthcare providers and their staff must be trained to respect and protect patient confidentiality. It should be a standard practice to verify that patient consent has been duly obtained before recording any data. Healthcare providers must communicate transparently with patients about data usage – why it is collected, how it is stored, and what protections are in place to secure its confidentiality and security. Patients are often willing to share information once they understand its purpose and safeguards. When patients experience ethical clinical practices, they extend that trust to how their data is handled.

Policymakers and regulators

The MoA should provide standard templates for privacy policy in multiple Indian languages and simplified consent forms to be used by clinics across the country. They should also establish clear grievance redressal

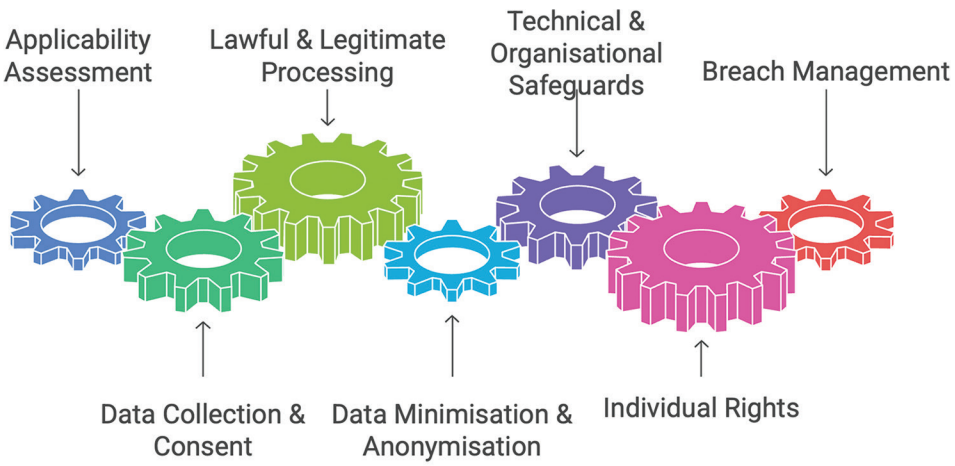

Figure 1: Digital Personal Data Protection Act 2023 compliance roadmap

mechanisms, including dedicated helplines, to address privacy-related complaints in Ayush services. Through the integration of privacy-preserving technologies, the MoA can enable large-scale AI innovation. In addition, measures including recognition or certification programs for "Privacy Champion" Ayush facilities could be introduced to recognize the efforts of Ayush facilities compliant with the DPDP Act. With support of the IndiaAI Mission, the MoA could lead interministerial coordination so that Ayush-specific data protection guidelines remain consistent with MoHFW and DPDP rules, avoiding confusing or conflicting compliance requirements.

Research institutions

Research institutions researching and building AI applications must develop expertise in data governance. As highlighted by the ICMR Guidelines, data privacy is a key concern when applying AI for biomedical research. Every proposal involving personal health data for research or development of AI applications must undergo privacy review alongside clinical ethics approval. In addition, the creation and use of synthetic datasets may be explored to facilitate data-driven innovation while protecting privacy. Further, as part of international collaborations, it is the key to ensure data sovereignty. Indian patient data should remain within Indian jurisdiction, with data-sharing agreements specifying permitted usage, security measures, and deletion protocols.

CONCLUSION

India is integrating centuries-old health knowledge systems into the digital era through platforms such as ABDM, Ayush Grid, AHIMS, e-Aushadhi, and telemedicine. These are strategic bridges between traditional wisdom and modern infrastructure. As India advances its leadership in both TM and emerging technologies, including AI, it has the opportunity to exemplify that progress and responsibility can and must coexist. Privacy-respecting and preserving AI solutions, particularly in Ayush, can become a hallmark of India's health innovation ecosystem.

Ayurveda's enduring relevance stems from its respect for individual care. In the digital age, that respect must be reflected through secure data practices, responsible AI, and transparent governance. Trust must be foundational to digital transformation. Sustainable digital health systems must embed privacy-by-design, ensure meaningful consent, empower citizens with data rights, and uphold transparency in AI deployment. The DPDP Act provides that foundation by establishing clear guidelines for data collection, processing, and protection, it creates the trust necessary for people to benefit from this digital transformation. Responsible development of digital systems can act as a catalyst for innovation, fostering trust among patients and confidence among practitioners. With these foundations in place, India is well-positioned to emerge as a global leader in responsible AI innovation in the health domain.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

REFERENCES

1. A Brief Guide on Ayushman Bharat Digital Mission (ABDM) and its Various Building Blocks. Delhi: National Health Authority, Ministry of Health and Family Welfare; 2021. Available from: https://abdm.gov.in: 8081/uploads/ABDM_Building_Blocks_v8_3_External_Version_eabbc5c0f3_4_a96f40c645_5716a684de_b344369144.pdf. [Last accessed on 2025 Oct 30].

2. Ayush Grid, the Emerging IT-Backbone for AYUSH Sector, to Integrate Operationally with the National Digital Health Mission. PIB, Delhi: Ayush. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1660936. [Last posted on 2020 Oct 02].
3. Ayur-Prakriti Web Portal. Available from: https://prakriti.ayush.gov.in. [Last accessed on 2025 Oct 30].
4. Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission, will Empower AI Startups and Expand Compute Infrastructure Access. PIB Delhi: Ministry of Electronics and IT. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2012375. [Last posted on 2024 Mar 07].
5. Anonymous. General Guidelines for Clinical Evaluation of Ayurvedic Interventions. 1st ed. New Delhi: Central Council for Research in Ayurvedic Sciences, Ministry of Ayush, Govt. of India; 2018.
6. Supreme Court of India. Justice K.S. Puttaswamy (Retd.) versus Union of India. 10 SCC 1; 2017. Available from: https://main.sci.gov.in. [Last accessed on 2025 Oct 30].
7. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Delhi: Ministry of Electronics and Information Technology (MeitY), Government of India; Enacted; 2023. Available from: https://www.meity.gov.in/static/uploads/2024 / 06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf. [Last accessed on 2025 Oct 30].
8. National Strategy for Artificial Intelligence. Delhi: NITI Aayog, Government of India; 2018. Available from: https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf. [Last accessed on 2025 Oct 30].
9. World Health Organisation. Mapping the Application of Artificial Intelligence in Traditional Medicine: Technical Brief; 2025. Geneva: World Health Organization; 2025. Available from: https://www.who.int/publications/i/item/9789240107663. [Last accessed on 2025 Oct 30].
10. World Health Organization. WHO–ITU–WIPO Showcase a New Report on AI use in Traditional Medicine; 2025. Geneva: World Health Organization; 2025. Available from: https://www.who.int/news/item/11-07-2025-who--itu--wipo-showcase-a-new-report-on-ai-use-in-traditional-medicine. [Last accessed on 2025 Oct 30].
11. Ayush Grid – My Ayush Integrated Services Portal. Ministry of Ayush, Government of India. [India]. Available from: https://maisp.ayush.gov.in/index. [Last accessed on 2025 Oct 30].
12. Ayushman Bharat Digital Mission Marks a Transformative Three-Year Journey Towards Enabling Digital Health. Ministry of Health and Family Welfare, Government of India. Available from: https://www.mohfw.gov.in/?q=en/pressrelease-87. [Last accessed on 2025 Oct 30].
13. NITI Aayog. Responsible AI #AIFORALL: Approach document for India, Part 1 – Principles for Responsible for AI. Delhi: NITI Aayog; 2021. Available from: https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf. [Last accessed on 2025 Oct 30].
14. IndiaAI Scales up Safe AI Efforts with Cutting-Edge Solutions for Deepfake Detection, Bias Mitigation and AI Penetration Testing. PIB Delhi: Ministry of Electronics and IT, Government of India. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2175698. [Last posted on 2025 Oct 07].
15. Indian Council of Medical Research. Ethical Guidelines for Application of AI in Biomedical Research and Healthcare; 2023. Available from: https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare. [Last accessed on 2025 Oct 30].
16. The Digital Personal Data Protection Act, 2023 – Section 6: Consent Provisions. Ministry of Electronics and Information Technology, Government of India. Available from: https://www.dpdpa.com/dpdpa2023/chapter-2/section6.html. [Last accessed on 2025 Oct 30].
17. Draft Digital Personal Data Protection Rules, 2025 – Rule 4: Rights of Data Principal. Ministry of Electronics and Information Technology, Government of India. Available from: https://www.dpdpa.in/dpdpa_rules_2025/dpdpa_draft_rules_english_.pdf. [Last accessed on 2025 Oct 30].
18. Digital by Design: DPDP Implementation. PIB Delhi: Ministry of Electronics and IT, Government of India. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2090271. [Last accessed on 2025 Oct 30].
19. Press Information Bureau. "DPDP Rules: Provisions for Significant Data Fiduciaries." PIB Delhi; Government of India; 2025. Available from: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2090271. [Last posted on 2025 Jan 05].
20. Khanna V, Kotwal A. Examining the significance of the digital personal data protection act, 2023 in the context of the healthcare industry: A comprehensive analysis. Discover Public Health 2025;22:381. Available from: https://link.springer.com/article/10.1186/s12982-025-00757-6. [Last accessed on 2025 Oct 30].
21. National Digital Health Ecosystem – Union Health Ministry has Adopted a Holistic Approach to Safeguard the IT System from Critical Security Threats Across Computational Layers. PIB Delhi: Ministry of Health and Family Welfare, Government of India. Available from: https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1942715. [Last posted on 2023 Jul 25].
22. National Digital Health Mission: Health Data Management Policy. National Health Authority, Government of India. Available from: https://abdm.gov.in: 8081/uploads/health_management_policy_bac9429a79.pdf. [Last accessed on 2025 Oct 30].
23. Report on AI Governance Guidelines Development. Ministry of Electronics and Information Technology (MeitY), Government of India. Available from: https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development. [Last accessed on 2025 Oct 30].
24. World Health Organization. WHO and HL7 collaborate to support adoption of open interoperability standards. Available from: https://www.who.int/news/item/03-07-2023-who-and-hl7-collaborate-to-support-adoption-of-open-interoperability-standards. [Last accessed on 2025 Oct 30].