



Strengthening India's healthcare ecosystem: Unlocking data governance in alignment with the Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025

Preface

Digital technologies have revolutionised the healthcare delivery system worldwide by enhancing the provision of quality healthcare, reducing workflow turnaround times, lowering overall costs and ushering in greater accountability. Digital health technologies have played a significant role in improving clinical outcomes and enabling the appropriate and efficient use of large volumes of data generated to streamline processes for healthcare providers and patients.

The National Health Policy (NHP) in 2017 provides a policy foundation for achieving 'Health for All' by using information and communication technologies to strengthen India's healthcare delivery systems through a patient-centric approach to optimal healthcare provision. The DPDP Act, 2023, along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) and other supporting laws, aims to protect patient data privacy in various healthcare settings. Despite these earlier efforts, the lack of a unified, comprehensive framework left significant gaps leading to personal health data breaches, which were eventually addressed by the enactment of the Digital Personal Data Protection Act, 2023.

In view of the Supreme Court's verdict on the KS Puttaswamy case in 2017, affirming 'privacy' as a fundamental right,^{2,3,4} the National Digital Health Blueprint (NDHB) was published in 2019,⁵ which was a comprehensive action plan for developing the applications of digital health technologies and outlined a strategic roadmap for digital health solutions.

Subsequently, with the launch of Ayushman Bharat Digital Mission (ABDM) in 2020, the National Digital Health Ecosystem (NDHE) was designed to be implemented in a mission mode based on the guiding principle: "Security and Privacy by Design" for the protection of personal digital data privacy, thereby complementing the Supreme Court's verdict. Thereafter, the ABDM published a health data management policy in 2022,⁶ which applied to all entities and individuals within the ABDM ecosystem.

In the context of the digitisation of the health sector, digital health interventions must comply with the DPDP Act, 2023 while ensuring accessibility, ease of use, efficiency and transparency in healthcare delivery. With robust digital data protection, India is ushering in a paradigm shift in healthcare management, rapidly closing in on its target of Universal Health Coverage (UHC).

The DPDP Rules, 2025, notified in the Gazette of India on 13 November 2025,⁷ have enabled India's healthcare ecosystem to undergo the most desired and significant regulatory transformation, long awaited, for the governance of every workflow in healthcare organisations in India under the DPDP Act, 2023.

Disclaimer

The market forecasts, projections, estimates and other forward-looking figures presented in this whitepaper have been sourced from third-party reports, research publications and other publicly available sources, as cited alongside the respective figures. These estimates are provided solely for informational and contextual purposes and reflect the assumptions, methodologies and information available to the respective third-party sources at the time of publication.

Such forecasts and projections are inherently subject to uncertainties, assumptions, market conditions and other factors that may cause actual outcomes to differ materially from the projected figures. The inclusion of any such estimates or projections in this whitepaper should not be construed as an endorsement, validation, guarantee or independent prediction by Deloitte of the achievement of the stated outcomes.

Deloitte does not warrant or guarantee the accuracy, completeness or future realisation of any third-party forecasts, projections or estimates cited in this whitepaper. Readers should refer to the original cited sources for the underlying methodology, assumptions, limitations and further context associated with such forecasts and projections.



Table of contents

Foreword	6	India's digital health ecosystem under the DPDP Act, 2023	34
Background	8	A. Futuristic vision for transformation in healthcare: Use cases of GenAI in the healthcare industry	35
Key elements	10	B. Formulation of an effective cybersecurity strategy to counter specific cyber threats in the health sector:	36
Evolution of digital healthcare	12	C. AI in traditional medicine: Aligning technological innovation with DPDP data governance	36
Impact of the implementation of the DPDP Act, 2023 and the DPDP Rules, 2025 in India	15	D. From digitisation to data governance: Navigating the digital-first healthcare shift	37
Potential positive impact at the individual level	16	Perspectives and call-to-action in the Indian healthcare sector	38
Potential positive impact at healthcare organisational level	17	Significance of the DPDP Rules, 2025 for successful implementation	41
Influence on pharmaceutical companies	19	Way forward for effective enforcement to promote India's digital healthcare	43
Impact on health insurance companies in India	19	Table 1: DPDP Act, 2023 compliance mapping of healthcare stakeholders	45
Conceptual impact of the DPDP Act, 2023 in India – Use cases	20	Table 2: Illustrative DPDP Act, 2023 compliance gap matrix	46
Use case 1: Behavioural changes of healthcare providers and patients	21	Deloitte's POV on the Imperatives to be undertaken by stakeholders under the ambit of the Indian healthcare ecosystem to operate and ensure all their actions are compliant with the DPDP Act, 2023 and the DPDP Rules, 2025	47
Use case 2: Streamlining processes for enhanced access through a patient-centric approach	22	Endnotes	49
Use case 3: Cross-border data sharing under the DPDP Act, 2023 and the DPDP Rules, 2025	24	Connect with us	52
Navigating vulnerabilities in data security compliance within the healthcare sector	26		
Digital healthcare regulation in India - The chronological context	26		
Data privacy governance: Challenges and DPDP Act, 2023 regulatory interventions	29		
Data sovereignty in the age of innovation: Bridging security gaps in			

Foreword



Joydeep Ghosh
Partner,
Leader – Life Sciences
& Health Care,
Deloitte South Asia

Healthcare in India is undergoing a significant technological shift, marked by the rapid introduction and steady application of various digital, robotic, biomedical, telemetry and other technologies in almost all aspects of healthcare delivery. This transformation is discussed in detail in Deloitte’s report, “The future of health in India”, published in April 2024 and launched at the Bharat Digital Healthcare Summit in New Delhi. In view of the National Health Policy 2017, which recognised the importance of information and communication technologies in strengthening healthcare delivery and promoting the vision of Health for All, initiatives such as the Ayushman Bharat Digital Mission have further accelerated the creation of an interoperable and citizen-centric digital health ecosystem. Under this framework, patient data in electronic form facilitates better clinical decisions, improves continuity of care and, consequently, clinical outcomes, strengthens public health programmes and supports evidence-based policymaking.

The scope, scale, magnitude and variety of patients’ personal health data collected, stored and processed by healthcare institutions make it one of the sector’s most valuable and sensitive assets, requiring continuous protection as India advances its technology-enabled healthcare transformation. The Digital Personal Data Protection Act, 2023, empowers the government of India to restrict the transfer of personal data to specified foreign states, thereby incorporating data sovereignty within the broader scope of national security.

The Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, establishes a key framework for responsible data processing, making digital healthcare more trusted, secure and citizen-centric. Healthcare organisations must therefore move beyond a predominantly compliance-led approach to a more integrated model of institutional data governance. This requires organisations to identify and address vulnerabilities across their data ecosystems, strengthen accountability and controls, and align people, processes, technology and governance structures with evolving data protection obligations.

As India ushers in a paradigm shift in healthcare management, the convergence of AI, advanced analytics, cloud technologies and interoperable digital health infrastructure will further increase the value of data and the complexity of associated risks. Responsible and sustainable data governance will consequently be central to enabling innovation while preserving individual privacy, security and trust. Healthcare organisations must internalise this framework in compliance with the DPDP Act, 2023, which serves as a regulatory intervention that requires competent institutional engineering to address vulnerabilities in data security compliance within the healthcare sector.

This white paper examines how healthcare organisations can transition from fragmented approaches to a comprehensive and sustainable data governance framework. It seeks to contribute to the development of a secure, responsible, interoperable and trusted digital healthcare ecosystem, placing the protection and stewardship of citizens’ data at the heart of India’s healthcare transformation journey.

Foreword



Joy Chakraborty
Chairman,
CII Hospital Tech 2026 and
Deputy Chief Executive Officer
P D Hinduja Hospital and Medical
Research Centre

India's healthcare sector is entering a new phase of transformation, driven by the need to deliver high-quality, accessible and patient-centric care at scale. As custodians of some of the most sensitive information an individual can share, including health records, diagnoses and personal histories, the sector has a unique responsibility to safeguard patient trust.

As healthcare becomes increasingly digital and AI-enabled, organisations are using data and technology to improve clinical outcomes, operational efficiency and patient experiences. This creates a defining imperative: to build a data ecosystem that is secure, compliant, efficient and worthy of the trust patients place in it.

At the Confederation of Indian Industry (CII) Western Region Sub-Committee on Healthcare & Lifesciences, we believe the sector stands at a pivotal juncture, as the DPDP Act, 2023, and the DPDP Rules, 2025, bring new clarity and rigour to how patient data must be protected, governed and used, including in the age of AI.

The impact of getting this right is significant: stronger patient trust, greater institutional resilience and healthcare organisations that are better equipped to innovate with confidence. Forward-looking organisations are already strengthening consent frameworks, breach management protocols and data accountability structures well ahead of enforcement timelines.

Through sustained industry dialogue, capacity-building and knowledge-sharing across hospitals, providers and technology enablers, the CII Sub-Committee remains committed to helping the sector navigate this evolving regulatory landscape with assurance. This white paper, developed in collaboration with CII and Deloitte India, provides a comprehensive and actionable roadmap across data governance, privacy, security, accountability, breach management and AI governance so that compliance readiness begins today.

Background



The Digital Personal Data Protection Bill (DPDP), 2023 was passed by both Houses of Parliament in August, 2023. Following the President's assent on 11 August 2023, it became the Digital Personal Data Protection Act (DPDP Act), 2023, providing a legislative framework for the protection of digital personal data and its lawful processing.

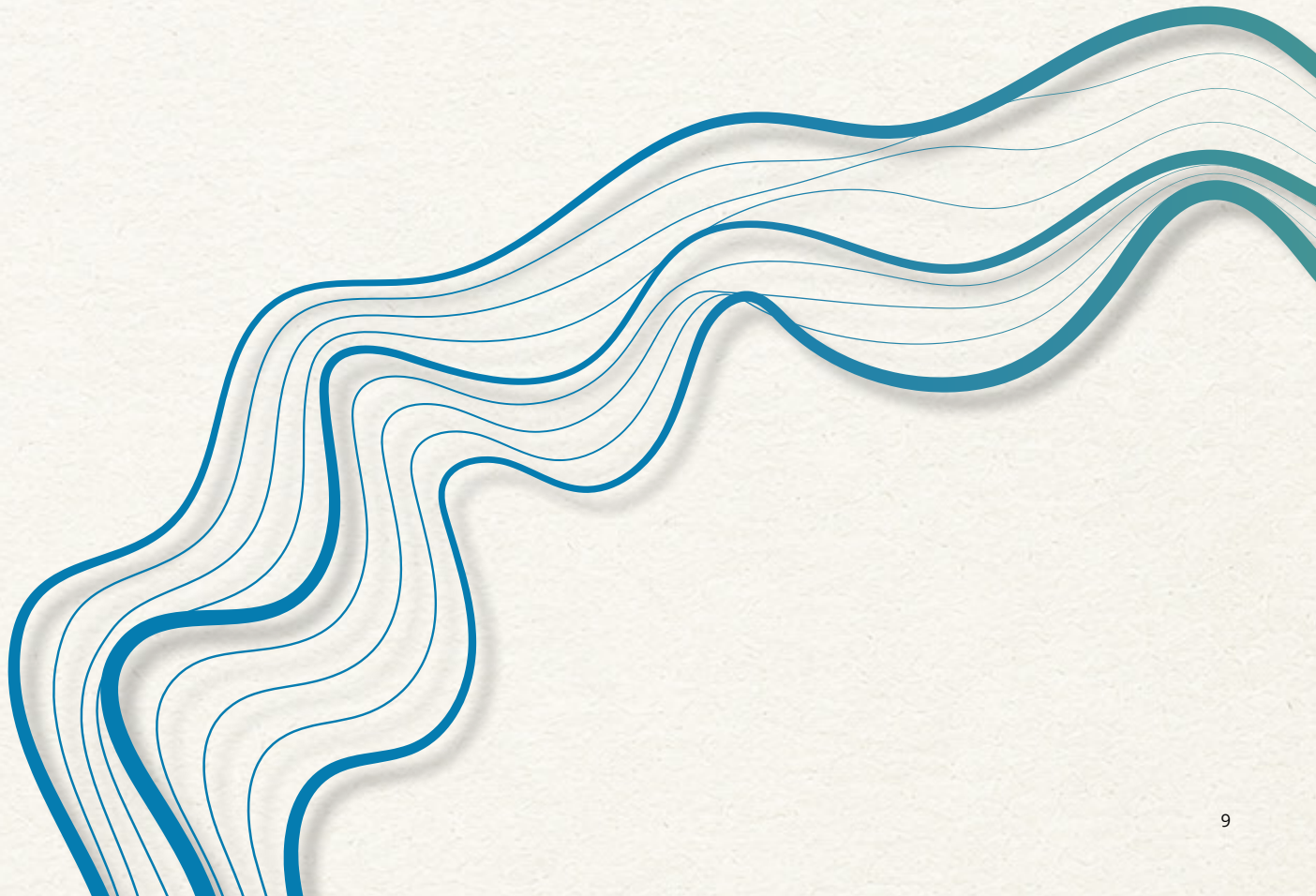
As the digital healthcare landscape evolves, the DPDP Act, 2023 is expected to play a vital role in data protection, including healthcare safeguarding patient information. By enhancing patient trust, improving data security and enabling responsible data sharing, these regulations contribute to a more secure and patient-centric healthcare environment.

“

An Act to provide for the processing of digital personal data in a manner that recognises the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

”

As the global digital healthcare landscape continues to evolve, India's healthcare sector is witnessing unprecedented growth in the adoption of technology-driven solutions. The emergence of numerous digital health technologies plays a significant role in improving healthcare access and outcomes. For instance, certain health- tech startups, innovative solutions in telemedicine, medical devices, diagnostics, use of artificial intelligence for personalised healthcare delivery, healthcare data analytics, etc., contribute largely to digital health services that not only immensely reduce the burden on physical health infrastructure and enhance patient health outcomes, but also help in redefining the healthcare delivery system in India.



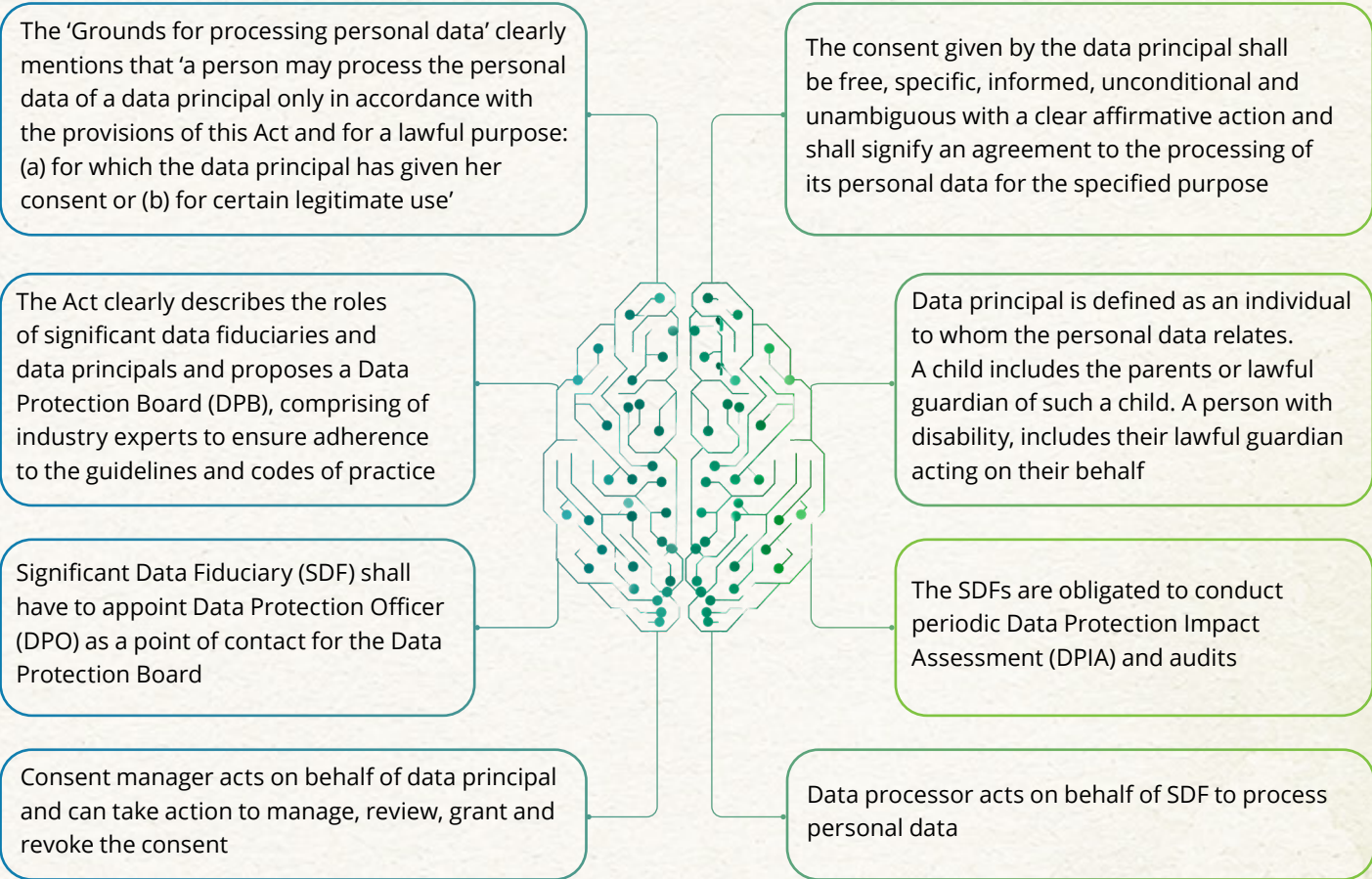
Key elements



The enactment of the DPDP Act, 2023 is revolutionary in safeguarding rights and duties related to digital personal data and protecting privacy at the individual and organisational levels. It will address the path for intentional digital data collection, storage and protection at the forefront, along with a strong consent-based data-sharing system.

In the context of the health sector, the DPDP Act, 2023 in India will play a vital role in safeguarding patient information by fostering a more secure, patient-centric healthcare environment, enhancing patient trust, improving data security and enabling responsible data sharing. Most importantly, it will empower the patients with direct access and control over their data.

Key elements of the DPDP Act, 2023



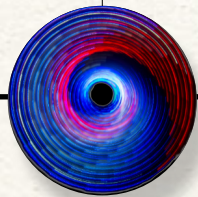
Evolution of digital healthcare

The global scenario

The evolution of digital healthcare has been a transformative journey spanning several decades. Here is a chronological overview of key milestones and developments in the global evolution of digital healthcare.

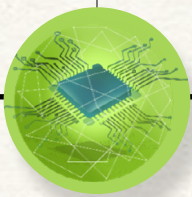
1960s–1970s: Emergence of health information systems

01 Early computer systems were used to manage administrative tasks in healthcare settings, such as billing and scheduling. The concept of Electronic Health Records (EHRs) began to take shape, although widespread adoption had not started.



2000s: Expansion of health IT

03 The 2000s marked significant growth in Health Information Technology (HIT) and EHR adoption, driven by government incentives in the US.



02

1980s–1990s: EHR systems

The 1980s saw the development of the first EHR systems, although they were often proprietary and lacked interoperability. The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, setting standards for the electronic exchange of healthcare data and ensuring patient privacy.



04

2010s: Mobile Health (mHealth) and wearables

The proliferation of smartphones led to the rise of these technologies.



2015s: AI and Big Data

05

AI and machine learning technologies were increasingly applied to healthcare for tasks such as diagnostics, drug discovery and predictive analytics. Big data analytics played a crucial role in identifying trends, improving patient outcomes and reducing costs.



06

2021s and beyond: Continued innovation

The COVID-19 pandemic accelerated the adoption of digital healthcare technologies, particularly telemedicine and remote monitoring. Virtual care and telehealth platforms saw explosive growth as people sought remote access to healthcare services. Health systems have been increasingly adopting interoperable EHRs, enabling better data sharing and care coordination. Consumer-oriented health and wellness apps and devices continue to expand, emphasising preventive care and health management.



The World Health Organisation (WHO) released a global strategy on digital health 2020–2027⁸ in December 2025 that provides a global policy framework for strengthening health systems through the application of digital health technologies for consumers, health professionals, healthcare providers and industry, with the broader objective of empowering patients and advancing the vision of 'Health for All' while supporting member states, particularly those with limited access to digital technologies, goods and services in building sustainable digital health capabilities.

As countries have progressively embraced digital transformation in healthcare, the need for robust privacy, data protection and governance frameworks has gained increasing prominence. These policies have been implemented by several countries across the globe and consequently developed or strengthened regulatory mechanisms to address the evolving challenges associated with the collection, processing, storage and exchange of health data. For instance, the European Union updated and strengthened its privacy laws through the General Data Protection Regulation (GDPR), which became applicable in May 2018.⁹

The adoption of digital healthcare has also accelerated, especially across Southeast and East Asia. For example, Singapore rolled out its National Electronic Health Record (NEHR) system in 2011 and subsequently progressed towards

cloud-based health data storage. Other countries, such as South Korea and Thailand, have also developed robust digital health models, demonstrating the growing integration of technology into healthcare delivery and health system management.

The evolution of digital healthcare has been shaped by global shifts toward standardised data protocols and digitised health records, pioneered by regulatory frameworks such as HIPAA for data privacy standards and various EHR incentive programs in Western healthcare. While understanding these international benchmarks is essential to contextualising the modern regulatory imperatives facing all healthcare providers, India has carved a unique evolutionary path by leveraging Digital Public Infrastructure (DPI) to achieve similar goals of interoperability and security through the Ayushman Bharat Digital Mission (ABDM), complemented by the data protection framework established under the DPDP Act, 2023.

This transition from global foundational logic to India's specific, technology-driven governance framework represents a significant milestone in India's digital health journey. This evolution is continuously shaped by regulatory shifts and demands patient-centred solutions that promise a future of continued innovation & empowered health management.



Impact of the implementation of the DPDP Act, 2023 and the DPDP Rules, 2025 in India

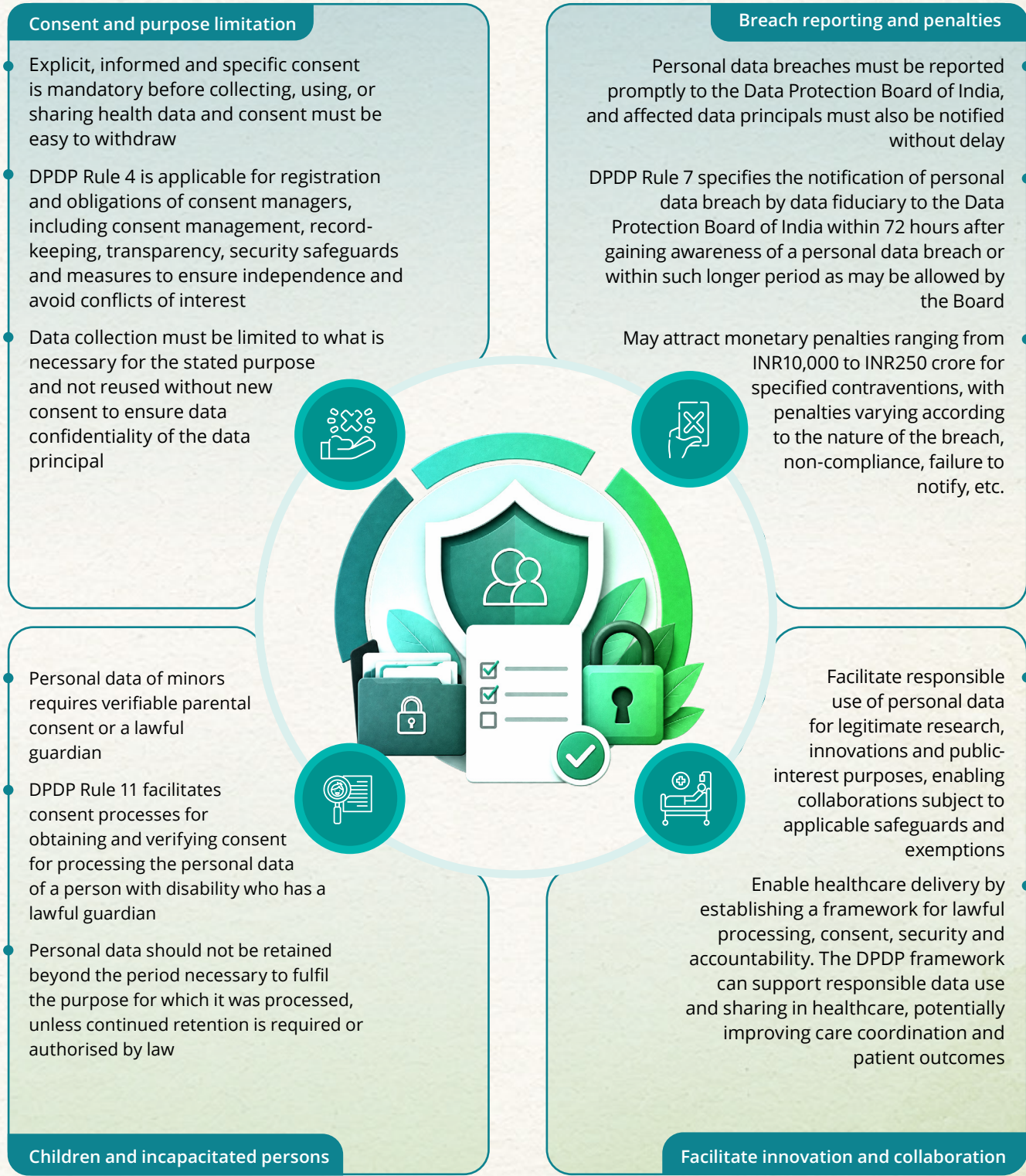


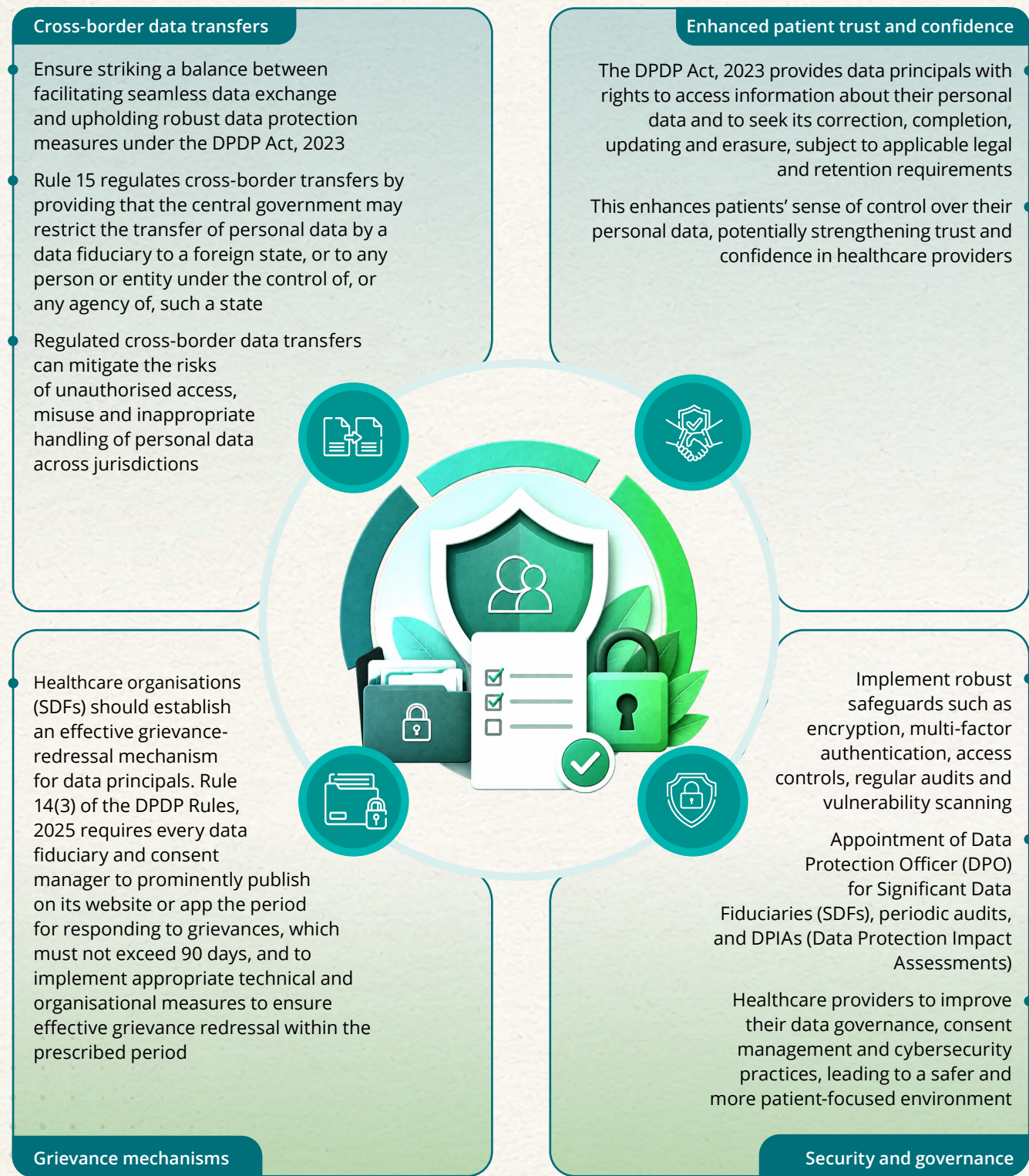
Potential positive impact at the individual level



Potential positive impact at the healthcare organisational level

Ensuring adherence to key compliance requirements by healthcare entities





Influence on pharmaceutical companies

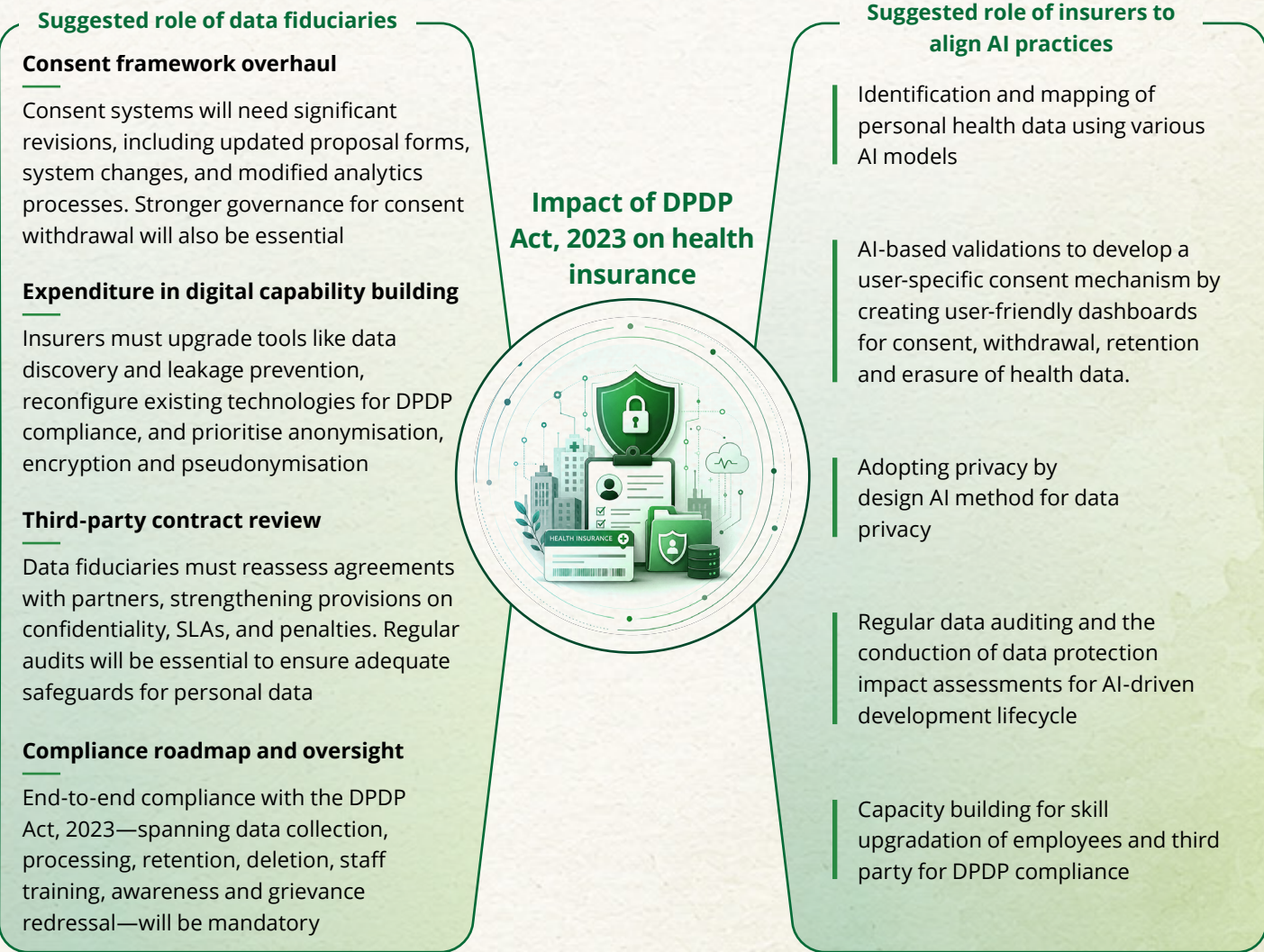
The DPDP Act, 2023, provides a regulatory framework for data protection, thereby ensuring that the pharmaceutical industry operates under strict oversight for the safe and effective delivery of goods and services.. By establishing a framework for responsible data processing and sharing, compliance with the DPDP Act can facilitate greater coordination between government and industry in implementing national health programmes and policies, while strengthening data governance, institutional

accountability, privacy protection, timely breach notification and grievance redressal, thereby fostering patient trust. However, ethical and operational concerns may arise from the close interdependencies between healthcare facilities and pharmaceutical companies, including drug supply, research collaborations, cross-border data transfers and financial relationships, which, if inadequately governed, can adversely affect patient care.

Impact on health insurance companies in India

Health insurers as data-intensive agencies: Health insurers can play a pivotal role by providing coverage for a wide range of wellness services and supporting community health initiatives. However, their operations involve multiple data fiduciaries and data processors that handle personal data, including third-party broking houses (both digital and

traditional), contractual agents, Third-Party Administrators (TPAs), marketing partners and users of insurance applications. This extensive data processing ecosystem underscores the need for robust data governance, clear accountability and appropriate privacy safeguards in accordance with the DPDP Act, 2023.



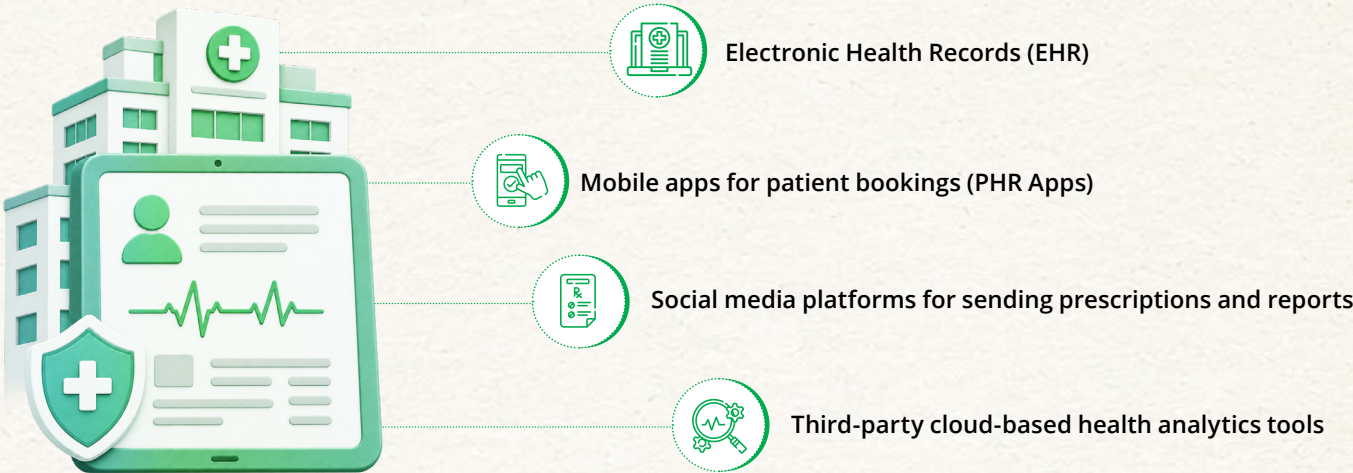
Conceptual impact of the DPDP Act, 2023 in India – Use cases



1. Illustrations of potential post-DPDP Act, 2023 positive impact at the organisational level

Use case 1: Behavioural changes of healthcare providers and patients

A multi-speciality hospital operates across several Indian States/UTs and uses the following applications and platforms:



Post DPDP Act, 2023, the scenario is expected to be:

Established consent culture

- Explicit, purpose-specific patient consent is now mandatory before collecting or processing personal data
- Front-desk and digital teams are now training to obtain records and track consent
- Systems are redesigned to request consent digitally, log revocation requests, and update access rights

Internal policies and SOPs

- Sharing reports
- Archiving data
- Deleting personal data on request
- Usage of social media platforms or email for sharing sensitive data is discontinued and replaced with secure patient portals or mobile-based PHR apps

Accountability mindset

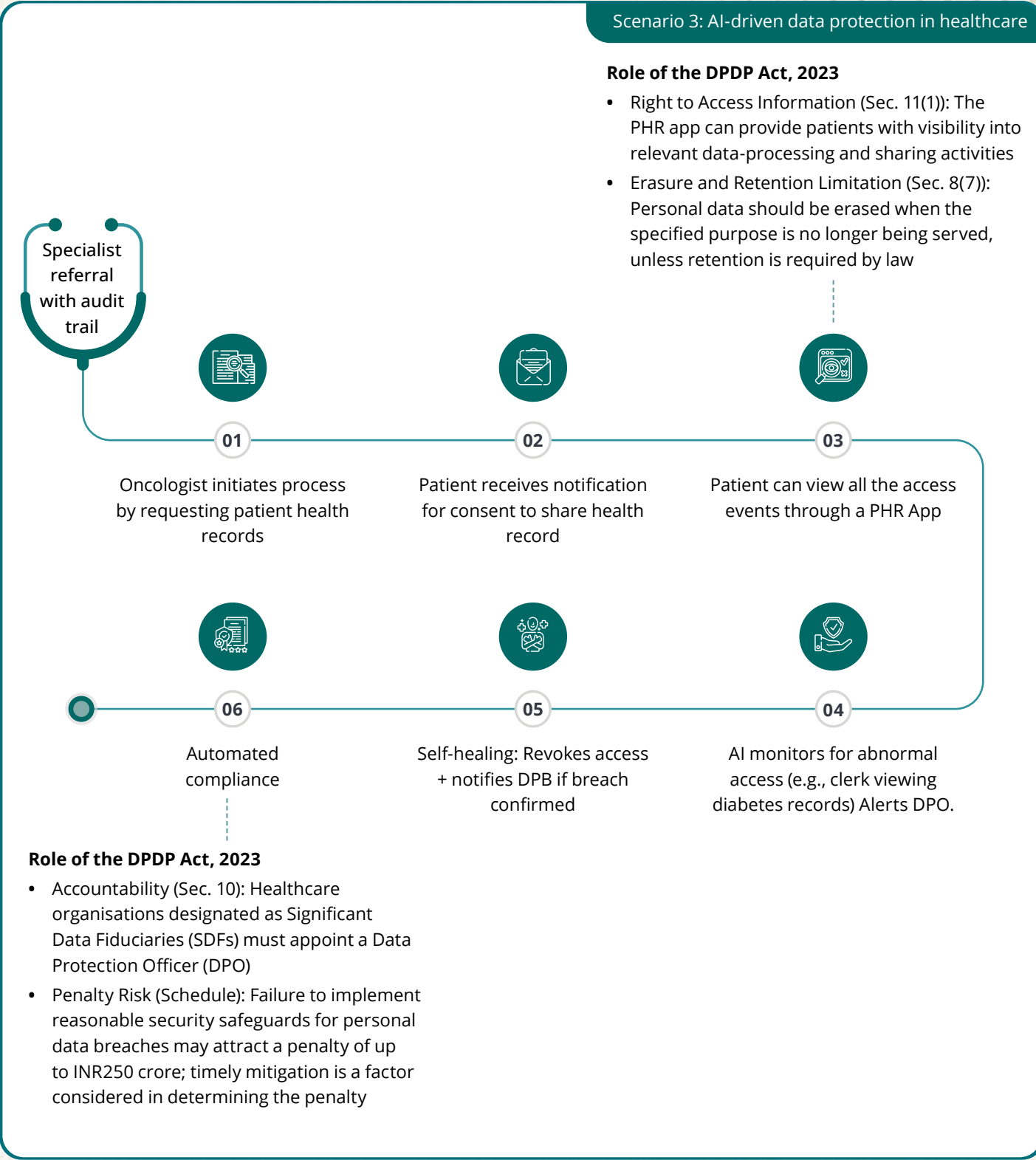
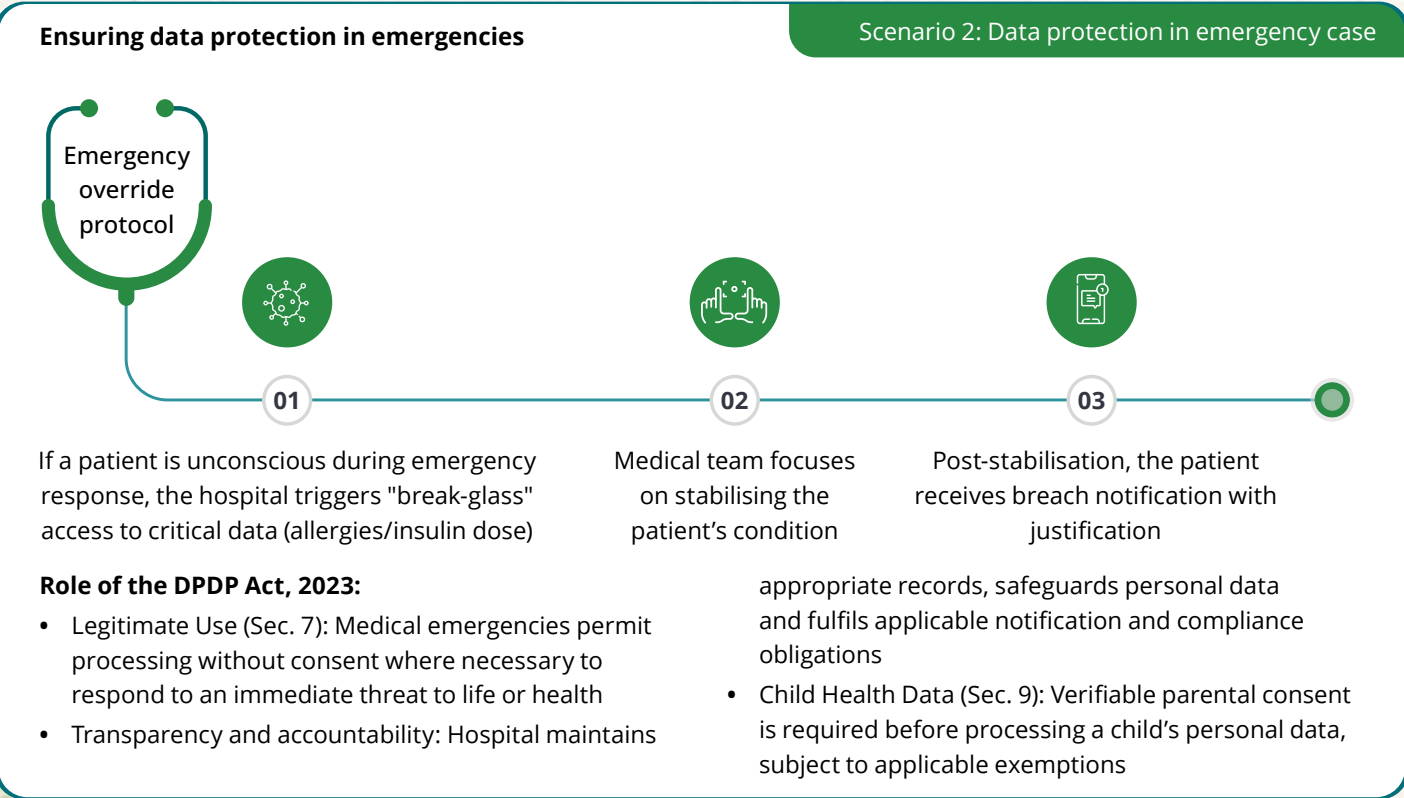
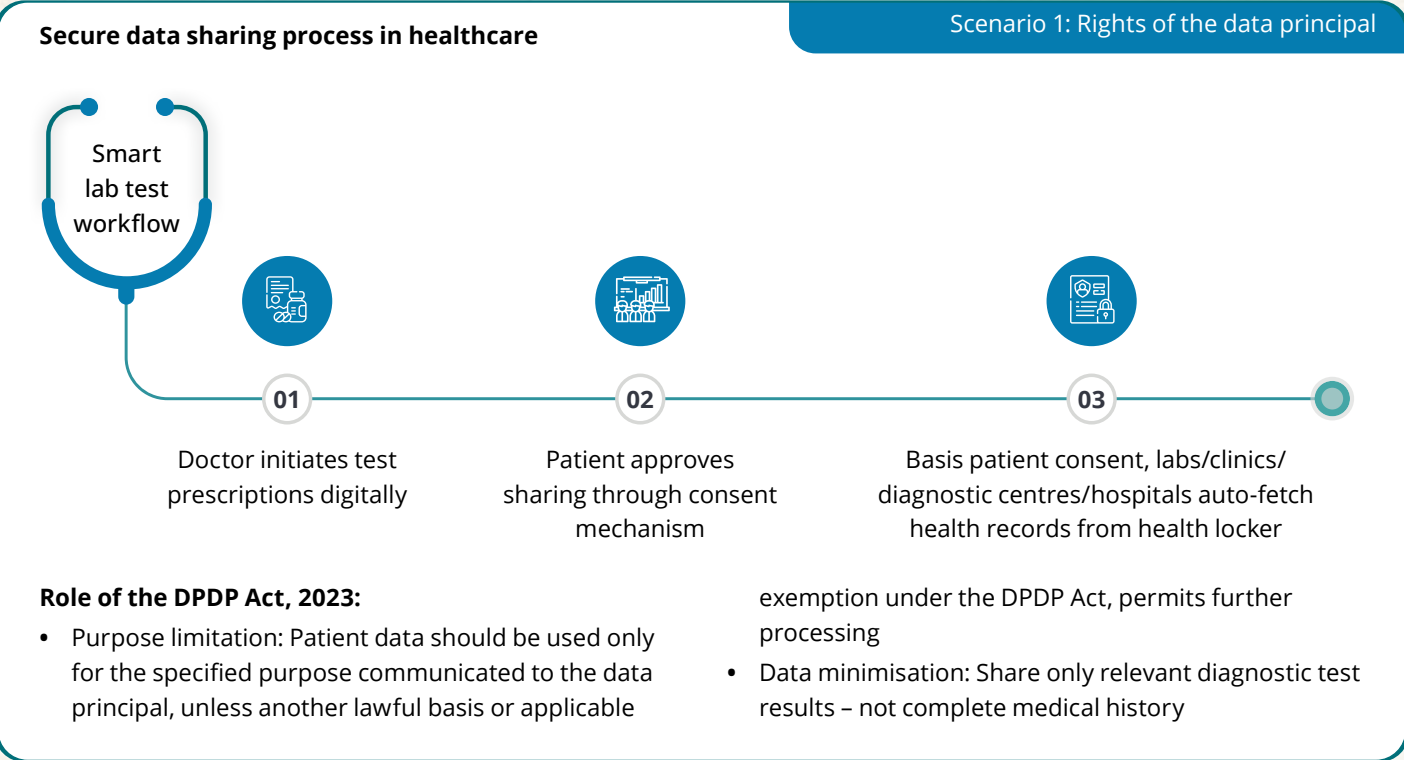
- Designated a Data Protection Officer (DPO) to ensure compliance across branches.
- Staff now report data breaches, even small ones, promptly, previously ignored.
- The IT team conducts regular audits and DPIA.
- Patient rights are given the due respect, and the staff mindset shifted from **“owning” patient data** to **“being a custodian of patient rights”**.
- Patients now request access to their data logs, correction of errors and deletion of old data

Data minimisation and purpose limitation

- The hospital stopped collecting non-essential data (e.g., education data for OPD registration)
- Behavioural shifts from **“collect everything just in case”** to **“collect only what’s necessary”**

Use case 2: Streamlining processes for enhanced access through a patient-centric approach

Due to the legal binding of the DPDP Act, 2023, the overall procedures have been formally streamlined, with enhanced access to affordable, user-friendly digital healthcare services and improved data security, confidentiality and privacy of health-related personal information, obtained through informed consent and for lawful purposes.

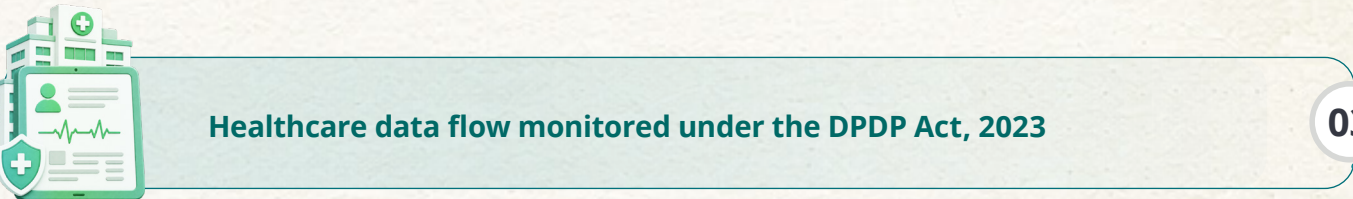
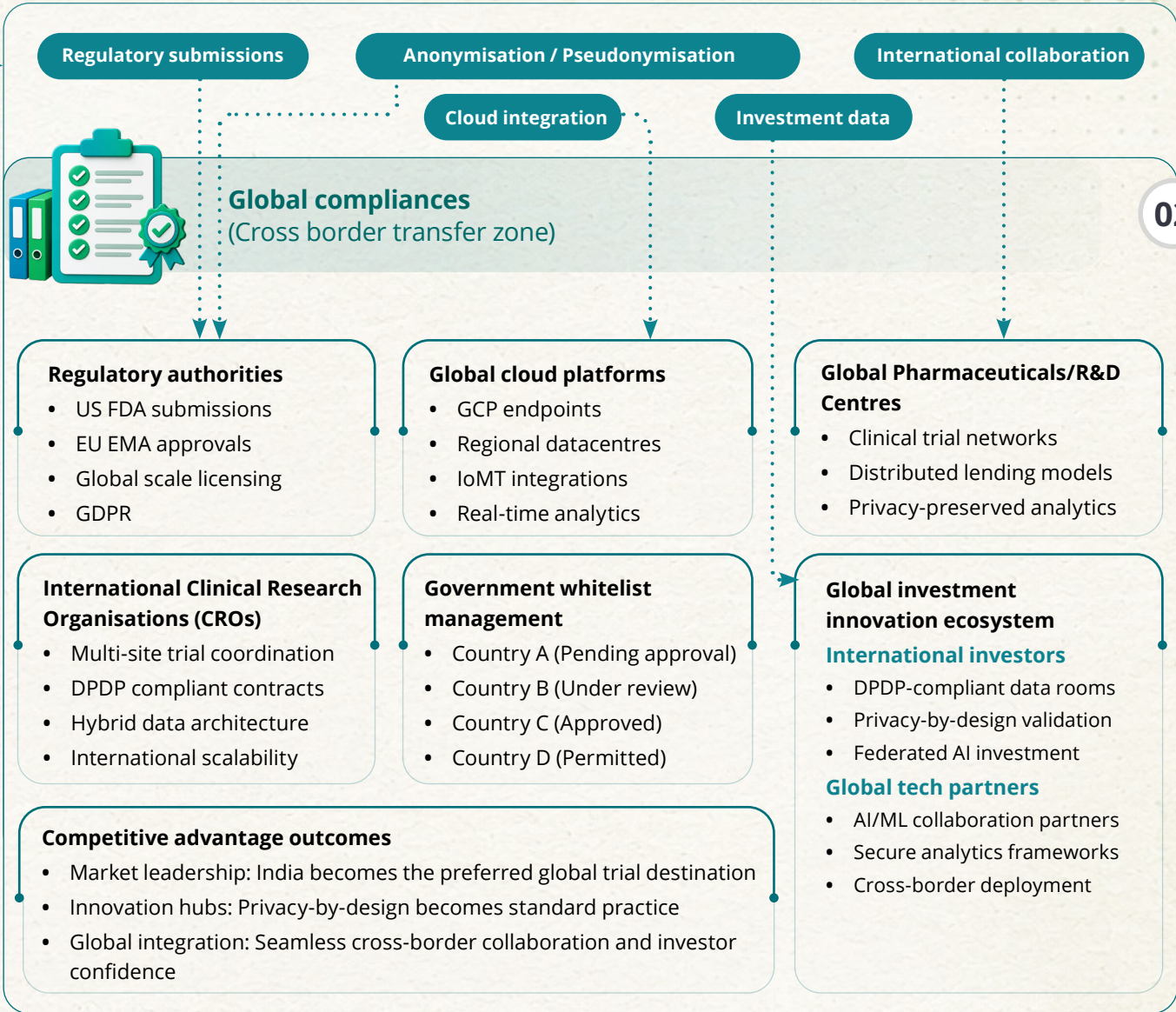
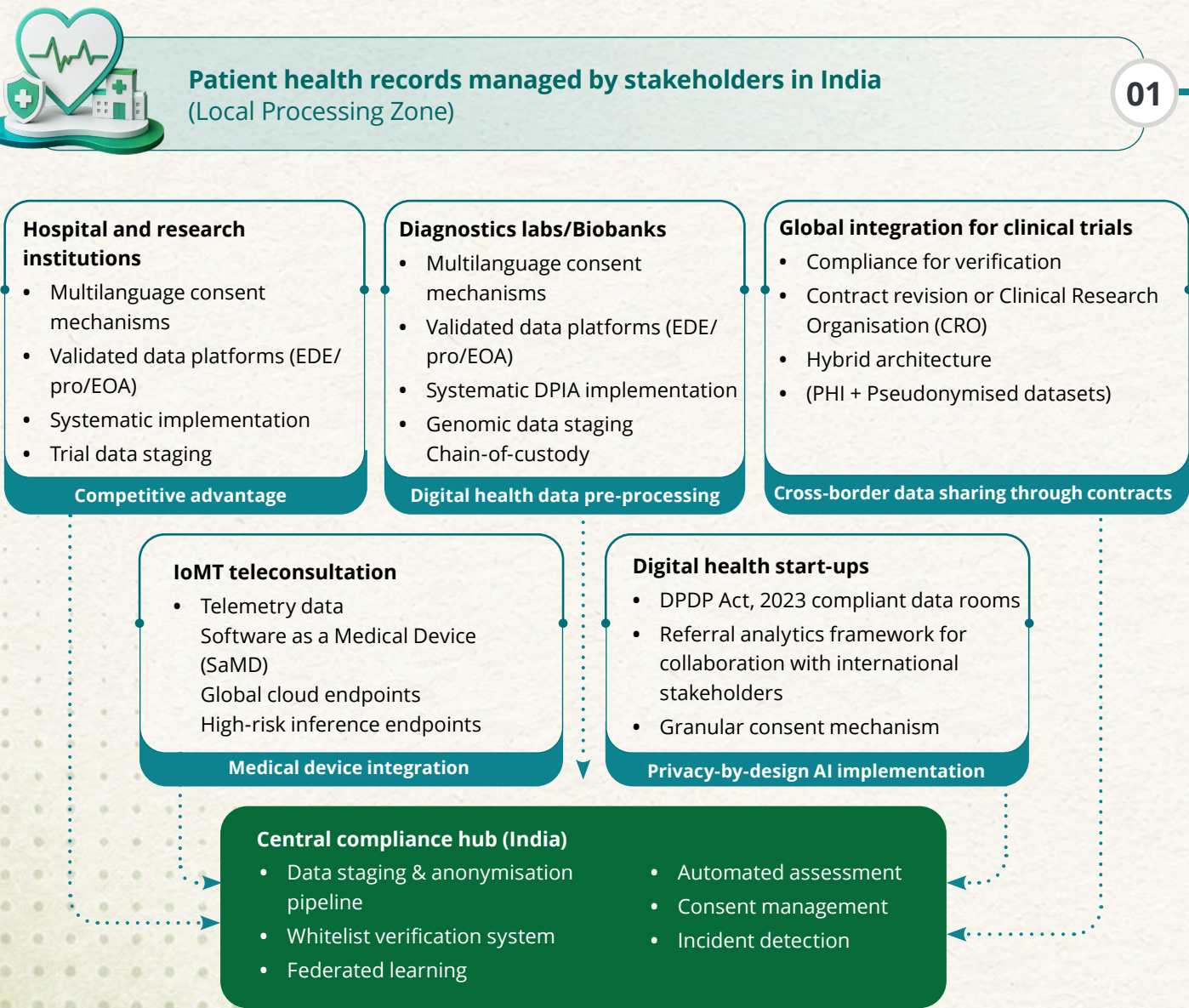


2. Facilitation of appropriate lawful cross-border data-sharing and promotion of international cooperation in medical tourism

India's medical tourism industry, estimated at US\$8.71 billion in 2025, is projected to reach US\$16.21 billion by 2030 at a CAGR of 13.23 percent, drawing over 4.5 lakh foreign patients annually.¹⁰ With world-class doctors and treatment costs nearly one-tenth of those in Western countries, India is a global hub for affordable, high-quality healthcare.¹⁰ However, as international patients share sensitive health data across borders, the DPDP Act, 2023 introduces stricter safeguards mandating secure consent, purpose limitation and cross-border data checks. Thus, boosting medical value travel must now balance growth with compliance, ensuring patient privacy travels as safely as the patient.

Use case 3: Cross-border data sharing under the DPDP Act, 2023 and the DPDP Rules, 2025
A patient from a foreign country shares past cardiac treatment records and insurance details with a hospital in India before travelling for surgery. Post-surgery, the Indian hospital needs to share treatment updates, discharge summaries and billing records with the insurance company of the patient's country of origin for claim settlement and with the patient's local physician for follow-up care.

Visual representation of cross-border healthcare data flow under the DPDP Act, 2023 and the DPDP Rules, 2025



Digital healthcare regulation in India – The chronological context



India has made significant achievements and advancements in the healthcare sector. These achievements covered a wide range of areas, from public health initiatives to medical research and innovation. Here are some notable achievements in the Indian healthcare sector:

- a. National Health Mission (NHM): India made significant progress in reducing maternal and child mortality rates primarily through programmes like 'Reproductive, Maternal, Newborn, Child, Adolescent Health and Nutrition (RMNCAH+N)', 'Janani Suraksha Yojana (JSY)', 'Intensified Mission Indradhanush (IMI)', 'Rashtriya Bal Swasthya Karyakram (RBSK)' and strengthening 'Health and Wellness Centres (HWCs)' for providing equitable healthcare delivery across India.
- b. Polio eradication: India achieved a historic milestone by being declared polio-free by the WHO in 2014.
- c. Tuberculosis control: India has been actively working to control the spread of tuberculosis (TB). The Revised National Tuberculosis Control Programme (RNTCP) expanded diagnostic and treatment services.
- d. Vaccine manufacturing and export: India is known for its vaccine manufacturing capabilities and has played a crucial role in producing vaccines for various diseases, including COVID-19 vaccines. The Serum Institute of India and Bharat Biotech, among others, were actively involved in vaccine production and distribution.
- e. Medical tourism: India has become a global hub for medical tourism, attracting patients from around the world for high-quality, affordable medical treatments. The country's healthcare infrastructure and skilled medical professionals have contributed to its reputation in this industry.
- f. Pharmaceutical industry: India's pharmaceutical industry is a major player in the global market, producing a significant share of the world's generic medicines. It has played a crucial role in making essential medicines affordable and accessible globally.
- g. Medical research and innovation: India's scientific and medical research community has made contributions to various fields, including drug discovery, genetics and clinical research.
- h. Telemedicine and digital healthcare: India has seen a surge in telemedicine and digital healthcare services, especially during the COVID-19 pandemic, making healthcare more accessible to remote and underserved areas. Cloud based 'eSanjeevani' platform (based on Hub-and-Spoke and patient to provider model), a National Telemedicine Service of MoHFW, was launched in 2019 as a step towards digital health equity which integrates Point of Care Diagnostic devices (PoCDs) to achieve Universal Health Coverage (UHC) thereby bridging the digital health divide (benefitting almost 14 percent senior citizens, irrespective of age, gender, family size

and covering almost 57 percent of female beneficiaries)¹¹

¹² (Source: MoHFW Annual Report 2025–26 & Press Information Bureau, January, 2026) demonstrating its role in promoting equitable and inclusive healthcare access. MoHFW released the Telemedicine Practice Guidelines in March 2020, thereby legitimising it in India.

- i. National Digital Health Mission (NDHM) or Ayushman Bharat Digital Mission (ABDM): It aims to make India 'Aatmanirbhar' or 'Self-reliant' in providing universal health coverage to all the citizens in the country. Aims to develop the backbone necessary to support the country's integrated digital health infrastructure. Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (PM-JAY) was launched in 2018, providing health insurance coverage to millions of low-income families.
- j. CoWIN (COVID-19 Vaccination Platform): India's CoWIN platform was developed as a nationwide digital platform to support the planning, registration, scheduling, administration and monitoring of COVID-19 vaccinations. It enabled citizens to register and book vaccination appointments, while providing healthcare authorities with real-time vaccination data, beneficiary tracking and digital vaccination certificates. The CoWIN platform demonstrated the potential of interoperable digital infrastructure to strengthen public health delivery, data-driven decision-making and equitable access to healthcare services.

Digitisation of medical data would be inclusive of the use of advanced computing sciences in 'big data', genomics and artificial intelligence, tools and services using information and communication technologies (ICT) for purposes connected to health for rendering (a) patient-centric digital health care and (b) achieving universal health coverage:

- i. Through efficient, accessible, inclusive, affordable, timely and safe manners.
- ii. Provides a wide range of data, information and infrastructure services.
- iii. Leverage open and interoperable standards-based digital systems, including Telemedicine, for enabling patients to receive medical care without physical access to a healthcare professional or facility.
- iv. Comprehensive legal framework for data-protection with a rights-based approach: The Supreme Court under Article 21 of the Indian Constitution unanimously reaffirmed the right to privacy in the 'Puttaswamy' case as a fundamental right. Hence, access to indigenous, socially and culturally relevant digitised healthcare, based on the principles of participation, accountability, non-discrimination, empowerment, legality, right to life, security, freedom, equality, autonomy, privacy and confidentiality was necessary.

It is important to note that healthcare challenges persist in India. Still, India's commitment to improving healthcare outcomes and addressing the healthcare needs of its diverse population has been praised by many countries. While digital healthcare was making strides, challenges such as data privacy, data security and regulatory compliance remained.



Data privacy governance: Challenges and DPDP Act, 2023 regulatory interventions



Challenges



Excessive collection of user-generated data and personal data of patients from digital platforms often leads to a threat of data exposure in the public domain



A critical compliance gap: May result in data principals unintentionally consenting to unnecessary data processing



Absence of privacy-centric policies: Results in health data breaches due to undermining of the need to maintain the privacy of data principals



Potential for unintentional public exposure: Through weak access controls and improper data management practices, which can result in personal data being made publicly available, thus posing reputational, legal and security risks



Massive increase in the market size of wearables in India (second-largest globally) generates sheer volumes of sensitive personal health data, raising grave concerns about misuse of data and violation of privacy

DPDP Act, 2023 intervention to overcome challenges



The principle of data minimisation outlined in the DPDP Act, 2023 specifies that only essential data be collected, limited to what is necessary for the stated purpose



Explicit, informed and specific consent is mandatory under the Act before collecting, using or sharing health data, and not be reused without new consent so that the confidentiality of the principal data is ensured



Imposes strict data security and privacy requirements through privacy-by design policy on data fiduciaries



On data leakage from prescriptions/video calls /cyberattacks, etc. users/data principals principals and the Data Protection Board should be informed immediately towards imposition of penalties and legal action by aggrieved patients



Require wearable manufacturers and digital health service providers to obtain free, specific, informed and unambiguous consent, through clear affirmative action, before processing users' health-related personal data for specified purposes (DPDP Act, 2023, Section6(1))

Challenges



Financial, reputational and strategic risks tied to data privacy lapses: With AI and analytics, the data fuels predictive diagnostics, drug discovery, telemedicine and insurance risk modelling



Data protection is a material risk factor across the healthcare value chain: Companies with weak compliance face regulatory penalties, reputational loss and capital setbacks



Investors treating privacy as a burden risk value erosion through heavy fines, licence suspensions and costly breaches that erode patient trust. Weak compliance can inflate costs, diminish valuations and derail IPOs or cross-border deals during due diligence



Direct sharing of diagnostic/lab data with insurers for claims assessment results in data breach: rising compliance costs (consent systems, audits, legal processes), risk of heavy penalties for improper data sharing and operational slowdowns if consent workflows are not efficient



Data-driven digital innovation, maintaining a balance between data conventionalisation for innovation and upholding patient privacy, remains a pivotal challenge

The online access provided by hospitals for consultations and reports, along with the use of mobile apps, portals, social media platforms, etc., is a major source of unregulated data leakage, thereby requiring adequate regulatory compliance in India's use of digital technologies to ensure

DPDP Act, 2023 intervention to overcome challenges



Secures policyholders' data while strengthening India's health insurance sector by embedding global best practices, building trust and positioning the industry for sustainable, globally competitive growth



Ensures that those embedding robust governance and privacy frameworks will be better positioned to capture investor trust, premium valuations and sustainable growth



Ensures that companies that incorporate trust and compliance into their core will scale as market leaders, treating data privacy as a strategic growth differentiator, with privacy audits, the appointment of DPOs, data mapping, breach response protocols and consent systems in place



Efficient consent management will be the differentiator between scalable, investment-ready insurers and those weighed down by compliance drag



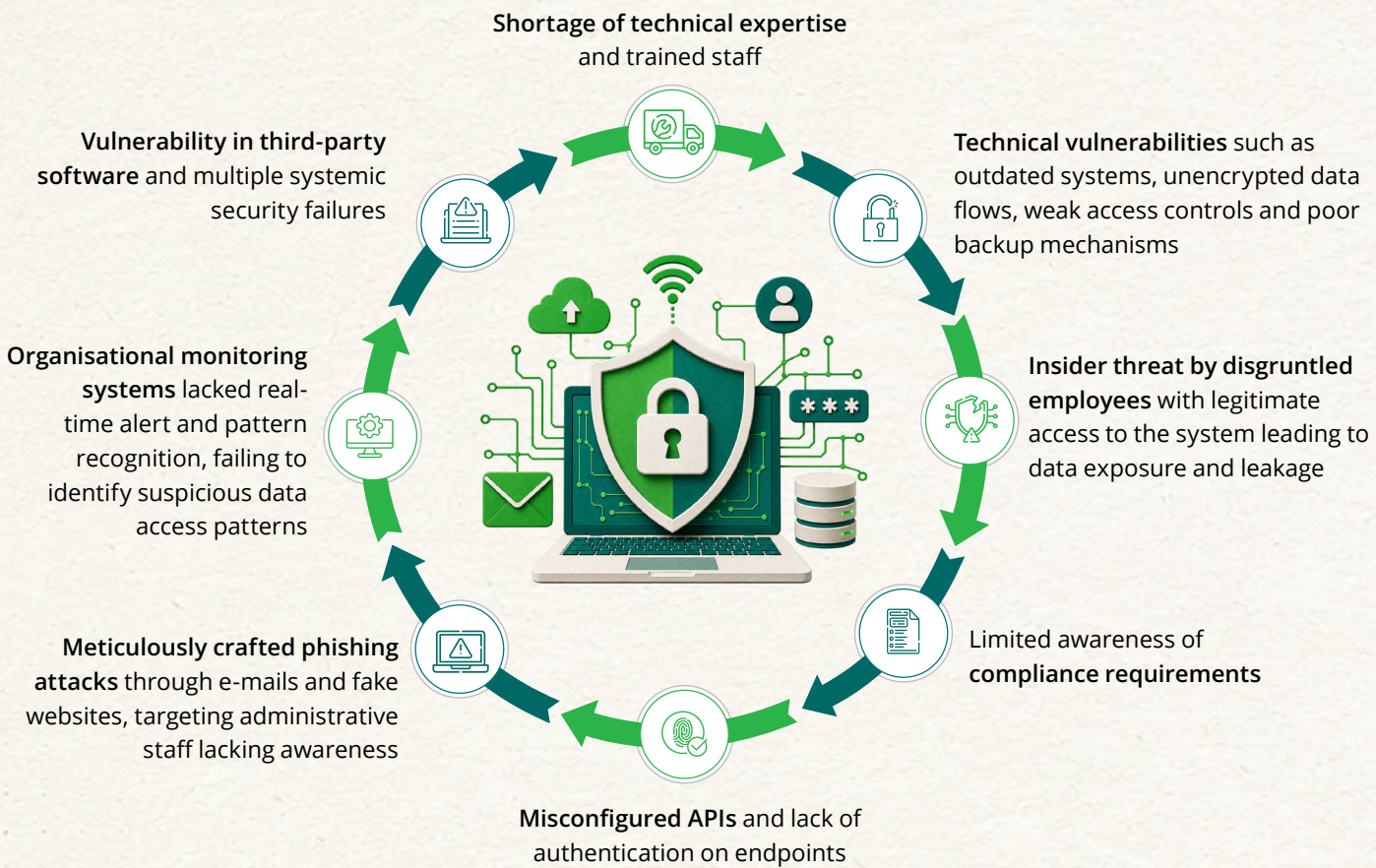
With robust data protection and clearly defined data exchange mechanisms, it enables researchers to tether patient data for personalised treatments

patient data privacy and good governance. Hence, a blend of the structural architecture of ABDM and the DPDP Act, 2023 and DPDP Rules, 2025 is required regarding appropriate data collection, processing, sharing and deletion.

Navigating vulnerabilities in data security compliance within the healthcare sector

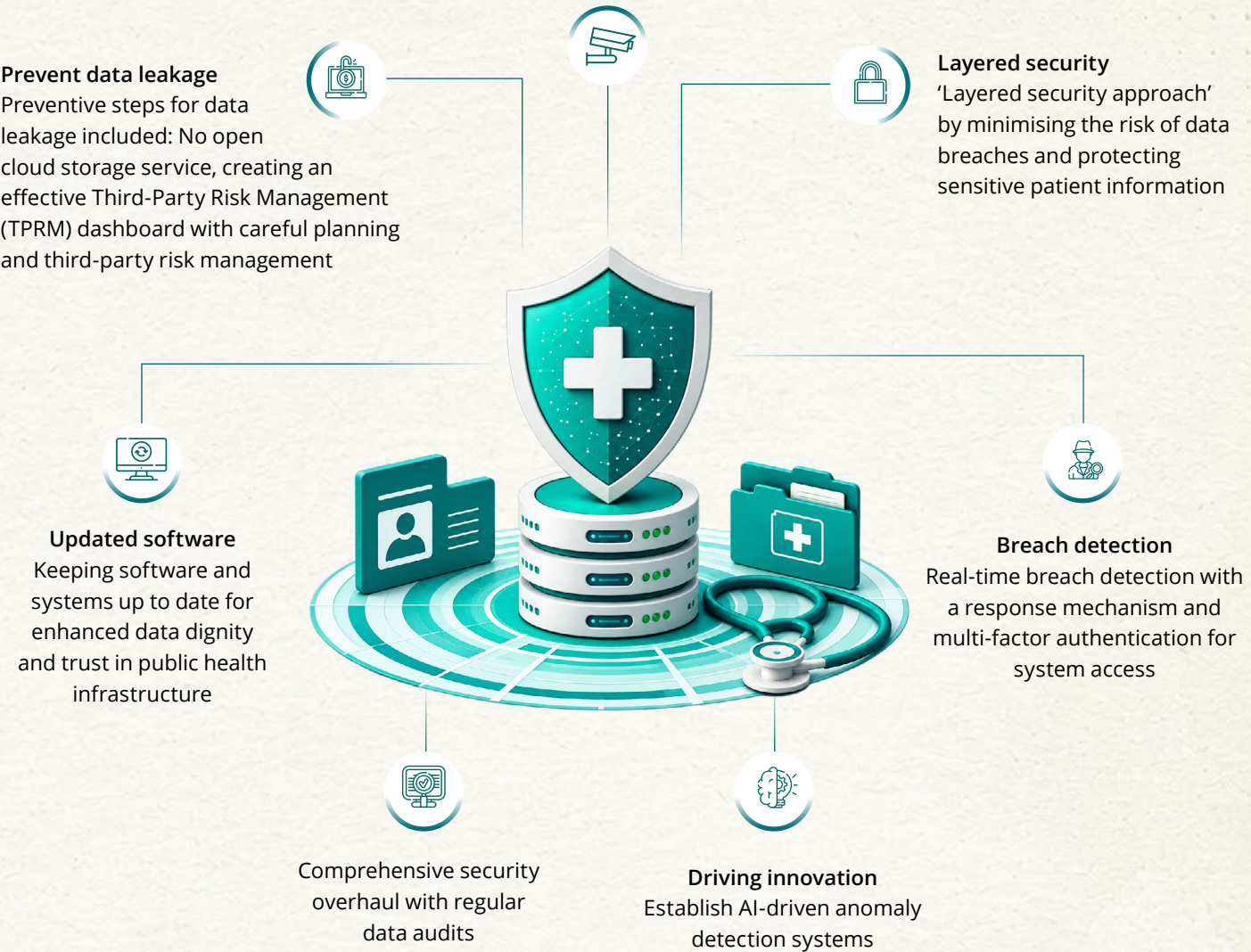
Data security standards in large hospitals and research-based healthcare entities in India conducting observational studies, drug trials, or health analytics that use personal data from EHRs, health registries, or biometric data from wearables reveal that, although the digitisation of health records has improved access and efficiency, it has also increased vulnerability to cyberattacks. For instance,

recent large-scale data breaches in the Indian healthcare sector have exposed the personal information of millions, highlighting systemic risks. As digital storage expands, breaches are becoming more frequent and sophisticated, thus creating systemic risks for patients and the healthcare ecosystem. The following gaps highlight the urgent need for stronger regulatory enforcement and structured compliance support across the sector.



Surveillance network

Creating a well-connected/integrated robust surveillance network linking epidemiological, genomic and clinical data, including humans, animals and the environment under 'ONE HEALTH MISSION' ensures institutional accountability and establishes a harmonised system for data collection, access, sharing, analysis and a unified data portal for infectious diseases



Data sovereignty in the age of innovation: Bridging security gaps in India's digital health ecosystem under the DPDP Act, 2023



Future threats demand measures such as quantum-resistant encryption, AI-driven threat detection, automated response and continuous audits to protect patient data. Generative AI can revolutionise healthcare by creating synthetic medical images and advanced diagnostic models, enabling clinicians to make informed decisions, aiding early detection of chronic conditions and addressing challenges posed by language diversity and limited workforce capacity. Synthetic datasets expand research potential, supporting precise and personalised treatments. Analysing electronic health records, AI can detect patterns and flag health risks. These capabilities enhance early diagnosis, timely intervention and better patient outcomes. Successful adoption depends on strong regulatory frameworks, with India advancing the ethical use of AI in healthcare.

A. Futuristic vision for transformation in healthcare: Use cases of GenAI in the healthcare industry

Voice to discrete data solution:
AI health device/machine-based collaboration

Description
Using voice recognition and NLP to label and categorise structured and unstructured audio data can help address major hospital management challenges. Beyond word detection, it interprets grammar, semantics and context to enable meaningful insights

Features

- Extract medical information from conversations
- Automates medical documentation for healthcare providers
- Browse available specialities and services at the hospital, check schedules and book online

Hospital operations & resource management: Optimising healthcare delivery

Description
AI agents can streamline scheduling, billing, recordkeeping and prescription refills while handling patient inquiries. They also automate onboarding, allowing staff to focus on critical tasks

Features

- Predictive admissions
- Bed management
- Staff scheduling
- Equipment coordination
- Emergency response
- Geospatial risk visualisation
- AI-powered outbreak detection
- Threshold-based alerting system

Drug discovery and development: Revolutionary impact on pharmaceutical research

Description
Pharma companies can use AI agents to speed up drug discovery and development by analysing compound libraries. They also build biomedical LLMs to summarise literature, trial data and patient profiles

Features

- Molecular design
- Target identification
- Virtual testing
- Cost reduction
- Microservices for building customised agentic workflow
- Predict cellular responses to drugs

Healthcare contact centre: Revolutionising overburdened health centres of states with AI agents

Description
Healthcare contact centres can use AI agents for virtual support, digital consultations, follow-ups and prescription reminders. They also guide patients to appropriate medical services efficiently

Features

- Patient inquiry management
- Insurance and billing support
- Appointment management

B. Formulation of an effective cybersecurity strategy to counter specific cyber threats in the health sector:

The vulnerability of EHR and medical IoT to quantum-scale decryption necessitates a proactive shift towards quantum-resistant frameworks. Protecting patient confidentiality and the integrity of medical services in this new era requires early alignment with national cybersecurity advancements. This transition is no longer merely a technical requirement but also a regulatory necessity to ensure that emerging healthcare technologies remain compliant with the data governance and mandates of the DPDP Act, 2023.

In response to these evolving risks, the Ministry of Electronics and IT (MeitY) has released a White Paper, titled 'Transitioning to Quantum Cyber Readiness', to prepare public systems for the 'Quantum Threat' to cybersecurity¹³. It provides a strategic roadmap to help public sector organisations prepare their cybersecurity frameworks for the emerging quantum computing era. It urged critical sectors, such as finance, defence and health, to prioritise the transition. India's roadmap for quantum-safe cybersecurity marks a vital step in securing national digital infrastructure.

With rising global quantum threats, adopting Post-Quantum Cryptography and fostering indigenous innovation are crucial to ensuring data integrity, cyber resilience and strategic technological sovereignty in the quantum era. MeitY launched QSim (Quantum Computer Simulator Toolkit) to facilitate cost-effective research in quantum computing for researchers and students.¹⁵ According to the 'Report on 'Quantum-Safe Ecosystem in India' released by the Department of Science & Technology, GoI, in May 2026, the key Indian initiatives on quantum technology are outlined below:

- National Quantum Mission (NQM): A INR6,003 crore mission (2023–2031) to build a strong national ecosystem spanning R&D, infrastructure, start-ups and skilled human resources.¹⁴
- Quantum Thematic Hubs (T-Hubs): Four verticals: Computing, Communication, Sensing & Metrology, Materials & Devices.¹⁴
- ISRO's QKD Test: Free-space Quantum Key Distribution demonstrated.¹⁴

C. AI in traditional medicine: Aligning technological innovation with DPDP data governance

The integration of AI into traditional medicine represents a transformative leap for global healthcare, offering unprecedented opportunities for diagnostics and clinical support. However, as AI models begin to ingest vast repositories of traditional knowledge and sensitive patient health information, the risks regarding data privacy and algorithmic bias become paramount. This evolution necessitates a rigorous integration of technological innovation and robust data governance frameworks, such as the DPDP Act, 2023.

Consequently, WHO released its first technical roadmap titled "Mapping the Application of AI in Traditional Medicine" on the use of Artificial Intelligence in traditional medicine, adopting India's proposal under the GI-AI4H initiative (which is a WHO-led International Platform for guiding to achieve safe, ethical and effective use of Artificial Intelligence), thus, recognising India's key digital initiatives like Traditional Knowledge Digital Library Unit (TKDL) and Ayurgenomics in the global framework. It is expected that the global

traditional medicine market size will likely cross US\$200 billion by 2030, given that over 80 percent of the world's population uses some form of traditional medicine (WHO).¹⁶

WHO's roadmap lays the foundation for a secure and inclusive AI transition in traditional medicine. The challenge now lies in balancing innovation with ethical safeguards for long-term global health integration.

The key features of the WHO strategy are as follows:

- Use case mapping: AI tools categorised into diagnostics, clinical support, text digitisation and public health.
- Governance principles: Includes transparency, safety, explainability, accountability and fairness in AI systems.
- Technical enablers: Emphasis on interoperable data sets, skilled workforce, regulatory frameworks.
- Innovation models: Encourage co-creation between AI engineers and traditional medicine.

As this AI-driven integration into traditional medicine

accelerates, the WHO's roadmap success will depend on establishing robust data governance frameworks that align with stringent regulatory mandates, such as India's DPDP Act, 2023, to ensure the privacy of sensitive traditional knowledge and patient data.

D. From digitisation to data governance: Navigating the digital-first healthcare shift

As India advances its digital health landscape, integrating emerging technologies into the National Health Mission (NHM) presents a transformative opportunity to modernise public health delivery. However, the shift towards a digital-first healthcare ecosystem necessitates a paradigm shift in how citizen data is managed, moving from simple digitisation to sophisticated data governance. For these technologies to truly bridge the gap between citizens and governance, the digital health tools must be compliant and anchored in the principles of privacy and accountability established by the Digital Personal Data Protection (DPDP) Act 2023.

Consequently, the use of emerging technologies in the healthcare system under the National Health Mission in India strengthens the enhancement of transparency, accessibility and efficiency in public health service delivery, which helps to bridge the gap between citizens and governance, thus making 'Aatmanirbhar Bharat', reflecting the strength, capability and a self-reliant healthcare ecosystem of a confident India in the 21st century through:

- India's rapidly expanding digital infrastructure with internet subscriptions surpassing 101.78 crore, mobile connectivity reaching over 98 percent of villages and more than 4.74 lakh 5G towers covering 99.6 percent of districts,¹⁷ has significantly accelerated digital healthcare adoption while increasing the scale and sensitivity of personal health data, reinforcing the need for robust privacy and data governance under the DPDP Act,.

- Building Digital Skills: PMGDISHA (Pradhan Mantri Gramin Digital Saksharta Abhiyan) Digital Literacy world's largest digital literacy initiatives focus on empowering people and institutions to use technology effectively, driving inclusive growth, strengthening digital governance and enabling citizens across the nation by supporting upskilling and building a self-reliant digital workforce. It was initiated to reach functional digital literacy in 6 crore rural households (one person per household) nationwide and has reached 6.39 crore individuals as of February 2026.¹⁷
- Breaking language barriers: BHASHINI-Sangraha (BHASHa INterface for India) is a pioneering initiative under the National Language Translation Mission (NLTM), aimed at bridging India's linguistic diversity through technology, which supports 36+ Indian languages, 350+ AI models and 23+ language services, as rural healthcare in India demands vernacular privacy notices to make the beneficiaries of rural areas self-reliant in seeking healthcare.¹⁸
- Strengthening Advanced Technology capabilities: 'IndiaAI Mission' aims to build a world-class AI ecosystem. Using India's global leadership in AI skills and GitHub contributions, the mission seeks to deepen AI and GenAI penetration within the healthcare delivery system. To manage emerging risks, the IndiaAI Safety Institute is being established as part of the mission's "Safe and Trusted" pillar.

Perspectives and call-to-action in the Indian healthcare sector



With India's digital health market

India's digital health market is projected to reach nearly US\$90 billion by 2034, registering a CAGR of 18.1 percent during 2026–2034. This sustained growth underscores the urgent need for healthcare providers to adopt robust governance and automated workflows to address gaps in digital literacy, interoperability and infrastructure. Tele-healthcare is the most lucrative technology segment registering the fastest growth during the forecast period, driven by rising adoption of remote consultations, AI-enabled diagnostics and connected care platforms (Source: India Digital Health Market Size Share, Trends and Forecast by Type, Component, and Region, 2026-2034).

India's digital health ecosystem has witnessed unprecedented growth through the convergence of Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB PM-JAY) and the Ayushman Bharat Digital Mission (ABDM). As of 2026, over 43.52 crore Ayushman Cards have been generated, including 1.14 crore Ayushman Vay Vandana Cards for senior citizens aged 70 years and above. The scheme is supported by a network of 36,229 empanelled hospitals (including 19,483 public hospitals), while the latest health benefit package offers cashless treatment across 27 medical specialities (Source: Press Information Bureau, Delhi, 2026).

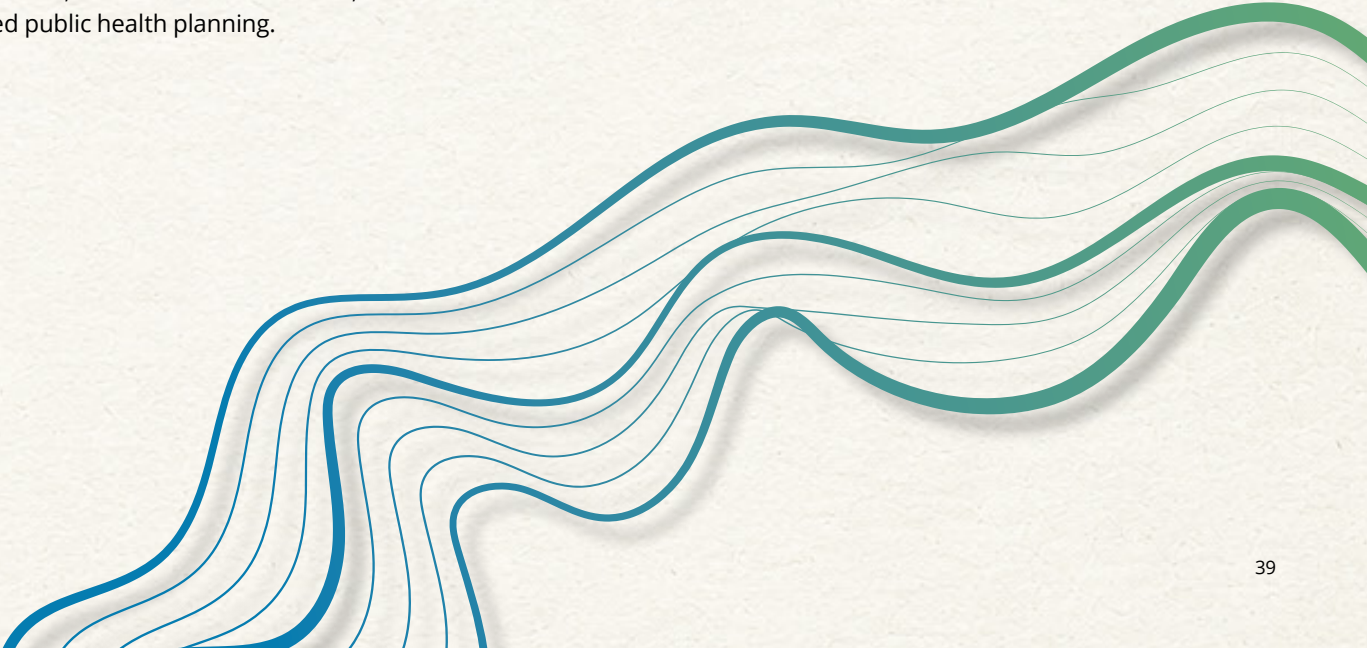
On the digital front, ABDM has enabled the creation of more than 90 crore ABHA (Ayushman Bharat Health Account) IDs and the linking of over 100 crore digital health records, with over 5 lakh healthcare facilities using ABDM-enabled software and over 9 lakh verified healthcare professionals (Source: ABDM Dashboard). These milestones demonstrate India's rapid transition towards a digitally integrated, interoperable healthcare ecosystem, creating a strong foundation for AI-driven healthcare, electronic health records, telemedicine and data-enabled public health planning.

Sector-specific adaptations are critical

Telemedicine has continued its rapid expansion in the post-COVID era, with digital consultations remaining significantly higher than pre-pandemic levels. India's national telemedicine platform, eSanjeevani, has completed over 482 million consultations by June 2026, demonstrating the growing reliance on virtual healthcare delivery (Source: Telemedicine Society of India). India's AYUSH ecosystem is witnessing rapid growth in 2026, driven by rising public investment and digital infrastructure. The Ministry of AYUSH's research ecosystem hosts 43,000+ research uploads with 2.45 million+ article views, reflecting stronger evidence-based adoption. With 30,900+ Ayurveda records, the sector continues to expand significantly (Source: AYUSH Research Portal, Ministry of AYUSH, GOI).

Rural healthcare demands vernacular privacy notices, given India's 22 official languages.

The adoption of the Internet of Medical Things (IoMT) and connected healthcare devices is accelerating across hospitals, diagnostic laboratories and remote patient monitoring ecosystems, underscoring the critical need for instant real-time data access in emergencies. India's medical devices sector is projected to expand to US\$50 billion by 2030 at a 16.4 percent CAGR (Source: Invest India, 2026), but the increased breaches underscore the urgency for Privacy Enhancing Technologies (PETs) such as homomorphic encryption.



Innovation drives compliance

Key insights from Deloitte on how innovation drives compliance

Several organisations, including Deloitte, have developed a variety of solutions to mature compliance risk management into a strategic advantage and make it more data- and technology-driven.

Deloitte's innovative solutions, such as 'RegTech' and 'RegMiner', are designed to simplify compliance management aligning with the DPDP Act, 2023 and DPDP Rules, 2025 in India.

The global Privacy-Enhancing Technologies (PETs)

Organisational readiness is vital

CXOs must lead compliance strategies, given penalties of up to INR200 crore for violations involving children's personal data under the DPDP Act, 2023. This includes conducting regular audits and breach simulations, while ensuring culturally adapted communication, multilingual consent notices and accessible privacy disclosures so that privacy information is understandable across India's diverse linguistic landscape, ultimately enabling patient-centric digital healthcare. Thus, adaptive governance frameworks are essential to address India's evolving healthcare ecosystem, where government health insurance coverage has expanded to 45.5 percent of rural households and 31.8 percent of urban households (Source: 'National Statistical Office (NSO) on Household Social Consumption on Health Highlights Transformative Progress in India's Healthcare System', Press Information Bureau, Delhi, 2026). This expansion has significantly increased the volume and sensitivity of digital health data, underscoring the need for structured oversight, equitable policymaking and robust privacy governance.

Digital healthcare transformation in India, in compliance with the DPDP Act, 2023, requires a collaborative effort between the government, healthcare providers, technology companies and other stakeholders. It is essential to prioritise patient-centred care, data security and regulatory compliance while harnessing digital technologies to revolutionise the healthcare sector.

market is experiencing rapid growth, expanding from an estimated US\$5.52 billion in 2026 to US\$14.3 billion by 2035, representing a CAGR of 27.4 percent (Source: Privacy Enhancing Technologies Market Report 2026 by 'The Business Research Company').

At the enterprise level, privacy has become a strategic business imperative: 99 percent of organisations report measurable benefits from privacy investments, 90 percent indicate that AI has expanded the scope of their privacy programmes and 93 percent plan to increase investments in privacy and data governance (Source: Cisco 2026 Data and Privacy Benchmark Study).

By prioritising these measures, healthcare entities can leverage the DPDP Act, to enable patient-centric digital transformation while mitigating privacy and cybersecurity risks. Such an approach aligns with the Government's INR350 crore budget allocation for the ABDM in 2026 (Source: 'Prioritising Healthcare for a Viksit Bharat 2047', Press Information Bureau, Delhi, 2026) and positions the sector to capitalise on the rapid expansion of India's digital health ecosystem, with the telehealth, remote patient monitoring and medical tourism markets projected to grow at CAGRs of 20.75 percent, 12.7 percent and 13.23 percent, respectively, through 2030. (Source: India Brand Equity Foundation (IBEF) Healthcare Report, 2026).

Ensure purpose limitation and lawful processing by mapping data flows, defining specific purposes and obtaining granular consent where required.

Significance of the DPDP Rules, 2025 for successful implementation



The DPDP Act, 2023 aims to provide the much-needed legal framework for ensuring the rights of protection and fair processing of digital personal data of each Indian citizen is intended to be implemented based on the 'digital-by-design' principle, thus paving the way for the creation of the platform proposed to be developed by the National Informatics Centre/Digital India Corporation.

However, the DPDP Rules, 2025, notified on 13 November 2025 and comprising 23 Rules and 7 Schedules, will play a

significant role in operationalising the DPDP Act, nationwide. The notification of the final DPDP Rules, 2025 provides extensive clarity and guidance to hospitals on time-specific operational mandates for transforming and managing patients' personal data.

At a glance: A few essential DPDP Rules, 2025 bearing great significance in the healthcare sector are listed below:



DPDP Rule 3: It signifies the importance of providing standalone, clear and plain language privacy notices, with an itemised description of the personal data being processed and the specific purpose(s) of processing. The organisations should ensure that such notices are contextualised and specific to healthcare services regarding demographic data, OPD cards, clinical laboratory reports, etc. and should not bear generalised information of patients.



DPDP Rule 4: It is applicable for the registration and obligations of consent manager with registration conditions prescribed in Part A of First Schedule and operational obligations set out in Part B of First Schedule in the Gazette of India. For the healthcare ecosystem, this will support structured, transparent and auditable management of patient consent across digital health services and data sharing arrangements.



DPDP Rule 7(2): The rule specifies the mandatory measure for personal data breach notification requiring Data Fiduciaries to intimate the Data Protection Board without delay upon becoming aware of a breach and provide updated and detailed information within 72 hours, unless a longer period is permitted by the Board.



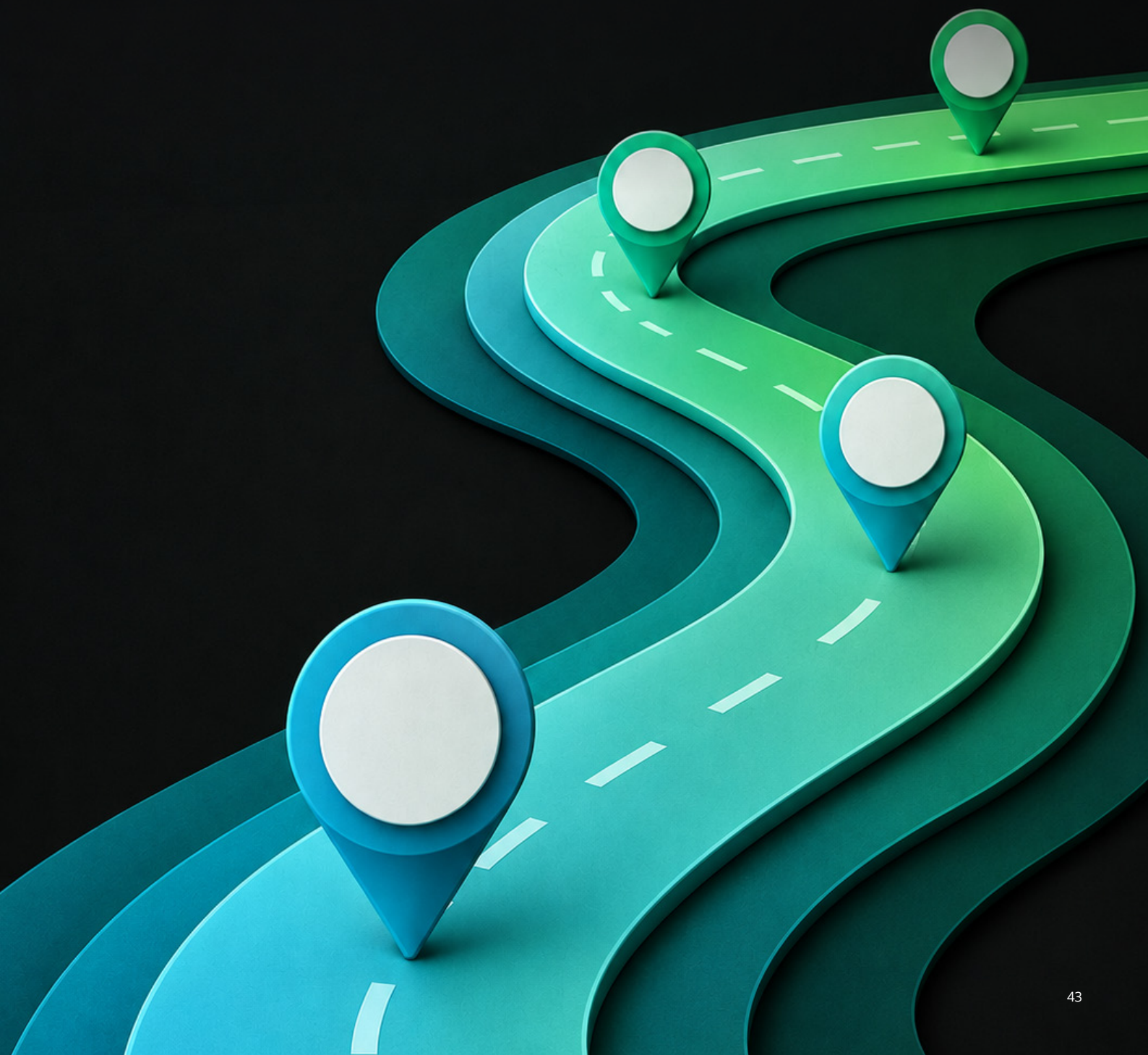
DPDP Rule 11: It facilitates verifiable consent for processing of personal data of person with disability (physical, mental, intellectual, sensory impairment, autism, cerebral palsy, mental retardation) who has lawful guardian.



DPDP Rule 12: It provides specified exemptions for processing children's personal data. Under Part A of Fourth Schedule, healthcare organisations and healthcare professionals may process such data, subject to specified conditions and only to the extent necessary for protecting the child's health or implementing a treatment and referral plan. Part B of Fourth Schedule covers specified purposes for processing such data, subject to prescribed conditions.

These final DPDP Rules, 2025 also indicate organisations for employee capacity building to implement data privacy processes and mandates necessary for compliance measures in alignment with the DPDP Act, 2023.

Way forward for effective enforcement to promote India's digital healthcare



To enhance the security posture of the healthcare ecosystem, researchers, security experts and healthcare organisations must focus on the following aspects and future strategic domains for seeking insight into and prevention of healthcare data breaches:

- Identify and address the main victims of cyberattacks on the healthcare sector.
- Undertake a study that investigates whether healthcare organisations are lacking usable security measures because of the absence of accountability and improper training of employees and clients.

- Classify hacking/IT incidents that led to healthcare data breaches.
- Identify preventive measures that should be taken to avoid healthcare data breaches.
- Harmonise policies with Ayushman Bharat Digital Mission (ABDM), India AI governance guidelines under IndiaAI Mission to ensure safe, inclusive & responsible AI adoption and ICMR's 'Ethical guidelines for application of AI in biomedical research and healthcare'.¹⁹

It is important to ensure that robust mechanisms are established to regularly update the technological advances and dynamism, for instance, the use of sensitive personal data to foster AI-driven innovations in the country.

The government's decision to seek public comments and suggestions, initiated on 5 March 2025, aimed to refine the Draft DPDP Rules, and address ambiguities in the DPDP Act, 2023. With the DPDP Rules, 2025 now formally notified in the Gazette of India on 13 November 2025, this consultative process has strengthened the credibility of the framework by ensuring greater clarity, transparency and accountability, particularly in relation to privacy notice obligations and other compliance requirements stipulated under the finalised rules.

The success of implementing the DPDP Act, 2023 depends on striking the right balance between flexibility and the standardisation of the rules laid down.

Compliance strategies of organisations related to: sector-specific issues,

- Development of mechanisms for uniform implementation rather than divergent compliance approaches, leading to incoherent, fragmented implementation virtually undermining the process for the establishment of consistency for data protection standards across the country,
- The digital ecosystem also needs to be assessed in the context of the DPDP Act, 2023.

The various stakeholders of the healthcare ecosystem must ensure certain fulfilment of obligations based on the key elements of the DPDP Act, 2023, as given below:

Table 1: DPDP Act, 2023 compliance mapping of healthcare stakeholders

Stakeholder	Data principals	Consent managers	Data fiduciaries	Data Protection Board (DPB)
Beneficiaries	• Exercise rights to access, correct and erase health records • Nominate representatives for health decisions	• Provide consent for health data sharing • Revoke/update consent across providers through unified interface	Not directly applicable (unless processing others' data)	• File complaints with DPB for consent/rights violations • Seek compensation for harm due to breaches
Hospitals/ Clinics	Not applicable	• Integrate systems with consent managers for real-time consent verification • Maintain audit trails of consent lifecycle	• Conduct DPIAs for sensitive processing (e.g., mental health data) • Implement encryption and breach response protocols • Appoint DPO for compliance oversight	• Report breaches within 72 hours • Face penalties (up to INR250 crore) for consent/security failures • Respond to DPB investigations
Diagnostic labs	Not applicable	• Verify patient consent through managers before processing tests • Link consent to specific purposes (e.g., tests vs. research)	Anonymise/pseudonymise datasets used for research: • Restrict data retention per test purpose • Validate third-party processor agreements (e.g., cloud labs)	• Demonstrate compliance during audits • Liable for penalties for unauthorised secondary use of health reports
Pharma companies	Not applicable	• Obtain fresh consent through managers for clinical trial participation • Segment consent for trial data vs. marketing	• Ensure transparency in drug safety surveillance • Implement role-based access to trial participant data • Conduct vendor risk assessments (e.g., CROs)	• Comply with DPB enforcement orders • Liable for unlawful processing of patient genetic data
Health insurers	Not applicable	• Use consent managers for policy underwriting & claims • Enable granular consent controls (e.g., sharing with hospitals)	• Obtain consent for fraud detection as a specified purpose, supported by internal risk control measures • Deploy tokenisation for sensitive health records • Conduct periodic security audits	• Respond to DPB inquiries about discriminatory pricing • Liable for penalties for non-consensual data sharing with intermediaries

Stakeholder	Data principals	Consent managers	Data fiduciaries	Data Protection Board (DPB)
Medical device manufacturers	Not applicable	Provide consent for real-time patient monitoring (IoT devices)	Secure by design; update firmware for vulnerability patches	Liable for insecure devices
Research institutions	Not applicable	Provide centralised consent for longitudinal studies	Ethics committee approval; publish anonymisation methodologies	Fines for re-identification attempts where there is a breach of an applicable DPDP obligation or prescribed research safeguards
Government agencies	Not applicable	- Use consent managers for public health programs (e.g., Ayushman Bharat) - Enable emergency bypass with DPB oversight	- Apply sovereignty exceptions judiciously (e.g., epidemics) - Publish data protection policies for schemes - Ensure state-level processor compliance	- Coordinate with DPB on national security exceptions - Subject of DPB scrutiny for mass surveillance programmes
Cloud/IT providers	Support fiduciary in enabling rights	Provide tools for consent manager integration	Act as data processors: Follow fiduciary instructions; no secondary use	Face direct liabilities for own DPDP breaches

Example: Stakeholders of the healthcare ecosystem may refer to the fulfilment of obligations based on the proposed regulatory reference and accountability framework:

Table 2: Illustrative DPDP Act, 2023 compliance gap matrix

Stakeholder	Gap description	DPDP clause violated	Gap severity scale	Owner assignment (Stakeholder-specific accountability)	Tentative timeline
Diagnostic labs	No consent manager integration	Sec 6(7)	Critical	Chief Technical Officer (CTO)	≤30 days
Health insurers	Unverified data retention	Sec 8(7)	High	Legal Head	≤60 days
Hospitals	Missing breach response protocols	Sec 8(6)	Critical	Chief Information Security Officer (CISO)	<45 days
Pharma companies	Clinical trial data shared with Clinical Research Organisations (CROs) and Data Protection Impact Assessment (DPIA)	Sec 8(2) Sec 8(3) Sec 10(2)(c)(i)	Medium	Data Protection Officer (DPO)	<120 days

Deloitte’s POV on the imperatives to be undertaken by stakeholders under the ambit of the Indian healthcare ecosystem to operate and ensure all their actions are compliant with the DPDP Act, 2023 and the DPDP Rules, 2025

Imperatives to be undertaken by stakeholders of the healthcare ecosystem



Every data fiduciary must conduct a customised assessment of their compliance strategies in sync with the company's or organisation's specific requirements. DPDP Act, 2023 key elements, such as consent managers and managing data principal rights, need to develop mechanisms to effectively notify Indian authorities of data breaches.



Developing and establishing a compliance strategy and provisioning a timeline for the implementation by the Data Protection Board and timely informing the affected data principal of the request.



Taking on board all the relevant stakeholders within the organisation by orienting them with the compliance strategy.



Conduct periodic Privacy Impact Assessments (PIAs) to identify and mitigate risks, particularly for high-risk processing activities.



Prioritising privacy compliance: Identifying all the personal data storage locations within the organisation.



Healthcare organisations need to ensure that the DPDP Rules, 2025, comprising 23 Rules and 7 schedules, will practically play a significant role in successfully making the DPDP Act, 2023 operational across the country.

DPDP Act, 2023 compliant organisations to focus on key areas with additional guidelines



Incorporate process-level steps for breach notification, stakeholder communication, data principal rights, consent management and processing of children’s personal data, including applicable exemptions under Rule 12 and Fourth Schedule of the DPDP Rules, 2025. Parents and guardians play a key role in safeguarding children’s personal data. Organisations should also consider restructuring internal teams to manage additional responsibilities, including coordination with the Data Protection Board, consent management and related digital services.



Update technical security measures, such as the use of virtual tokens, in accordance with the suggestions under the draft Rules.



Establish robust mechanisms to regularly update the technological advances.



Implement sector-specific issues and removal of ambiguities through clarity of privacy maintenance rules.



Conduct a reassessment beyond the existing assessment results to ensure compliance with the draft Rules, including communication and reporting mechanisms, notices or any other alignment per the draft Rules.



Strike the right balance between flexibility and standardisation of the laid Rules for successful implementation of the DPDP Act, 2023 to prevent data breach and maintain data security, privacy and dignity of data principal.

The DPDP Act, 2023 is considered to bring about the first significant digital revolution in Indian healthcare. It is expected to play a vital role in safeguarding patient information by: (a) enhancing patient trust, (b) improving data security and (c) enabling responsible data sharing, thus contributing to an assured and secure patient-centric healthcare environment.

The successful implementation of the DPDP Act, 2023 will depend on the clarity of its provisions, effective enforcement mechanisms and the readiness of organisations to comply with the new requirements. Continuous stakeholder engagement and capacity-building initiatives will be crucial in addressing challenges and ensuring a smooth transition to the new data protection regime.

The DPDP Act, 2023 represents a pivotal advancement in safeguarding individual privacy, with relevance to the healthcare sector. The multifaceted impact includes strengthening patient trust, enhancing data security, encouraging global collaborations and driving innovation. However, the DPDP Act, 2023 also necessitates rigorous compliance measures and substantial investments in data governance and cybersecurity infrastructure. Adopting the DPDP Act, 2023 is essential to strike a balance between privacy and progress, ensuring that healthcare remains a

secure, reliable and forward-looking domain where patient welfare is prioritised in the digital era.

The final DPDP Rules, 2025 have introduced operational requirements that are mandatory for all healthcare organisations to follow for effective health service delivery, in alignment with the mandates of the DPDP Act, 2023. The notification of the final DPDP Rules, 2025 provides extensive clarity and guidance on operational mandates that are time-specific for transforming and managing patients' personal data.

Compliance audits for India's DPDP Act, 2023 are essential for organisations that collect, process, or store personal data of individuals in India. By conducting regular audits, organisations can protect individual privacy, mitigate legal risks, enhance their reputation, prevent data breaches and maintain trust in the digital economy.

In summary, the DPDP Act, 2023 and the DPDP Rules, 2025 act as a guiding roadmap for healthcare service delivery, bearing in mind the data privacy of patients, forming the basic framework for a patient-centric approach for a digital health ecosystem to build patient trust and commitment for legal obligations by healthcare organisations towards personal data safety and privacy in India.

Endnotes

1. Ministry of Health and Family Welfare, Government of India, National Health Policy 2017, <https://www.mohfw.gov.in/>
2. K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (Supreme Court of India, 24 August 2017), https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India
3. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., W.P. (Civil) No. 494 of 2012 & connected matters, Supreme Court of India, 26 September 2018, <https://indiankanoon.org/doc/127517806/>
4. 'Fundamental Right to Privacy', Justice K.S. Puttaswamy v Union of India, <https://www.scoobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/>, 2023.
5. National Digital Health Blueprint, Ministry of Health and Family Welfare, 2019, https://www.nrce.in/download/files/pdf/National_Digital_Health_Blueprint_Report_comments_invited.pdf
6. Draft Health Data Management Policy ver 2.0 published under Ayushman Bharat Digital Mission (ABDM) by the National Health Authority (NHA) in Apr 2022 - https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf
7. The Gazette of India PART II — Section3 — Sub-section(i) NEW DELHI, THURSDAY, NOVEMBER 13, 2025/KARTIKA 22, 1947 REGISTERED NO. CG-DL-E-14112025-267650 MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY New Delhi, the 13th of November 2025/Kartika 22, 1947.
8. World Health Organization (WHO), Global Strategy on Digital Health 2020–2027, Geneva: World Health Organization, 2025, ISBN 978-92-4-011687-0, <https://iris.who.int/server/api/core/bitstreams/a64d584f-015b-471f-9d86-9ea263cfb516/content>
9. Dipika Jain, "Regulation of Digital Healthcare in India: Ethical and Legal Challenges," Healthcare 11, no. 6 (2023): 911, <https://doi.org/10.3390/healthcare11060911>, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10048681/>
10. India Brand Equity Foundation (IBEF), Healthcare Industry in India, February 2026, <https://www.ibef.org/industry/healthcare-india>
11. Ministry of Health & Family Welfare, Annual Report 2025–26., https://notto.mohfw.gov.in/WriteReadData/Portal/News/951_1_Annual_Report_of_the_MoH_FW_2025_-_2026.pdf
12. Press Information Bureau, Ministry of Health & Family Welfare, January 2026, <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jan/doc202611749801.pdf>
13. MeitY's Whitepaper on Quantum Cyber Readiness: "Transitioning to Quantum CyberReadiness", <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADV01&CACODE=CICA-2025-3410>, written by CERT-In, SISA & Ministry of Electronics and IT (MeitY), July 12, 2025.
14. Department of Science & Technology (DST), Ministry of Science & Technology, Government of India, National Quantum Mission (NQM), May, 2026, <https://dst.gov.in/sites/default/files/Quantum-Safe-Ecosystem-in-India.pdf>
15. Press Information Bureau (PIB), Ministry of Electronics & Information Technology, Government of India, "QSim – Quantum Computer Simulator Toolkit", August 2021, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1749667®=48&lang=2>
16. World Health Organization, "Mapping the application of artificial intelligence in traditional medicine: technical brief," July 11, 2025, <https://www.who.int/publications/i/item/9789240107663>
17. Press Information Bureau (PIB), Government of India, "Lok Sabha Starred Question No. 169," 11 February 2026, <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2226569®=3&lang=1>
18. Press Information Bureau (PIB), Ministry of Electronics & Information Technology, Government of India, "Digital India BHASHINI Division: National Hub for Language Technologies Powers End-to-End AI at Population Scale," 12 March 2026, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2239132&lang=1®=3>
19. Indian Council of Medical Research (ICMR). Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare. New Delhi: Indian Council of Medical Research; 2023. ISBN: 978-93-5811-343-3, <https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare>

20. The Gazette of India PART II — Section1 NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA) REGISTERED NO. DL—(N) 04/0007/2003—23 MINISTRY OF LAW AND JUSTICE (Legislative Department) New Delhi, the 11th of August 2023/ Sravana 20, 1945 (Saka).

21. The Gazette of India, Extraordinary, PART II — Section3(i), NEW DELHI, FRIDAY, JANUARY 3, 2025/PAUSHA 13, 1946 REGISTERED NO. CG-DL-E-03012025-259889 Ministry of Electronics and Information Technology (MeitY) New Delhi, the 3rd of January 2025/Pausha 13, 1946.

22. 'The Digital Personal Data Protection Act, 2023 – The Inconspicuous Absence of Legitimate Interest', Abhishek Mitra, Bar Bench, 21 Aug 2023.

23. India's Draft DPDP Rules,: Leading Digital Privacy Compliance, January 2025 <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-indias-draft-dpdp-rules-2025-noexp.pdf>

24. 'Digital transformation, From a buzzword to an imperative for health systems', 26th October 2021, Maulesh Shuklaetal,<https://www2.deloitte.com/xe/en/insights/industry/healthcare/digital-transformation-in-healthcare.html>

25. 'THE FIRST DIGITAL REVOLUTION IN HEALTH CARE', V. Srinivas Deputy Director Administration AIIMS, New Delhi, 2015.

26. 'Digital Transformation- Key research findings'- Health systems consider digital capabilities a path to fundamentally transform their relationship with consumers, <https://www2.deloitte.com/xe/en/insights/industry/health-care/digital-transformation-in-healthcare.html>

27. Release dated 9 Aug 2023 on Salient Features of the Digital Personal Data Protection Bill, 2023 by Ministry of Electronics & IT, Government of India - <https://pib.gov.in/PressReleaselframePage.aspx?PRID=1947264>

28. Article dated 11 Aug 2023 published by Deloitte India on Key provisions, Enforcement and Implementation of the DPDP Act, 2023 - <https://www2.deloitte.com/in/en/pages/risk/articles/the-digital-personal-data-protection-act-2023.html>

29. 'The Impact of DPDPA on Healthcare, Ensuring Patient Privacy in the Digital Era', K.S.S Shruthi, October,07,2024,<https://ezovion.com/the-impact-of-digital-personal-data-protection-act-on-healthcare-ensuring-patient-privacy-in-the-digital-era> 'Navigating Data Privacy Compliance in India: A Comprehensive Guide to DPDPA 2023 Compliance Audits,' November 16, 2023, <https://secureprivacy.ai/blog/india-dpdpa-2023-compliance-framework>

30. Ayushman Bharat Digital Mission 'DATA PRIVACY POLICY', Ministry of Health and Family Welfare and National Health Authority, (<https://abdm.gov.in> website: <https://abdm.gov.in/abha-PRIVACY-POLICY>).

31. THE CHALLENGES AND IMPACT OF PRIVACY POLICY COMPREHENSION, Korunovska et al. / Privacy Policy Comprehension: Vienna University of Economics and Business, Vienna, Austria, Twenty-Eighth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco.

32. Privacy and Healthcare Industry: The Impact of the DPDP Act, 2023, October 2023,www.tsaaro.com

33. e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, OpenAccess, Fully Refereed International Journal) Volume:05/Issue:01/January-2023 Impact Factor-6.752 www.irjmets.com [www.irjmets.com@International Research Journal of Modernization in Engineering, Technology and Science \[1880\]](mailto:www.irjmets.com@International Research Journal of Modernization in Engineering, Technology and Science [1880]).

34. FUTURE PANDEMIC PREPAREDNESS AND EMERGENCY RESPONSE: A Framework for Action' Report-of-the-Expert Group-Future- Pandemic-preparedness Niti Aayog pg 32-33, 65-66, AUGUST 2024 Health Division. 100 Days Mission Implementation Report by International Pandemic Preparedness Secretariat (IPPS); <https://d7npznmd5zvwd.cloudfront.net/prod/uploads/2023/01/100-Days-Mission-2nd-Implementation-Report-1.pdf>

35. Business Standard, "80% digital healthcare investment rise in 5 years in India: Jitendra Singh", Business Standard, 16 June 2022

36. The Economic Times HealthWorld, "84% healthcare providers to increase digital solutions budget in next 12 months: Survey", 14 February 2023

37. PIB Delhi, "ECONOMIC SURVEY HIGHLIGHTS THRUST ON RURAL DEVELOPMENT", Ministry of Finance, 23 January 2023

38. RURAL HEALTH STATISTICS 2020-21, MINISTRY OF HEALTH & FAMILY WELFARE [Online]. Available: https://main.mohfw.gov.in/sites/default/files/rhs20-21_1.pdf [Accessed 1 May 2023]

39. Elsevier Health, 'Clinician of the Future" [Online]. Available: https://www.elsevier.com/data/assets/pdf_file/0004/1242490/Clinician-of-the-future-report-online.pdf [Accessed 1 May 2023]

40. World Health Organization, Regional Office for South-East Asia, "The Decade for Health Workforce Strengthening in the SEA Region 2015–2024: mid- term review of progress" [Online]. Available: <https://apps.who.int/iris/bitstream/handle/10665/333611/sea-rc73-7.pdf> [Accessed 1 May 2023]

41. Swarajya, "Gujarat: World's First Telerobotic Surgery Performed By Dr Tejas Patel From 32 Kilometres Away", 7 December 2018

42. United Nations, "India to overtake China as world's most populous country in April 2023, United Nations projects", 24 April 2023

43. Office of the Principal Scientific Adviser to the Government of India, "IIT Madras Develops Blockchain-based Healthcare Information Systems for MobileApps", 9 April 2021

44. The New Indian Express, "Health infrastructure in Budget 22, a missed opportunity", 17 March 2022

45. Prabhat Prakash, "Are smart wearables creating a connected health ecosystem?", EHealth World, 21 October 2022

46. The Print, "DRiefcase launches 'Healthy Bytes' to simplify healthcare for you", The Print, 10 October 2022

47. The Economic Times HealthWorld, "Indian healthcare sector should tap emerging opportunity in health tech: Amitabh Kant", 28 March 2022

48. Centers for Disease Control and Prevention, U.S. Department of Health & Human Services, "Well-Being Concepts", 31 October 2018

49. The Economic Times HealthWorld, "Docty to set up 100 digital health kiosks across Telangana, Andhra, Maharashtra", 12 April 2022

50. Empowering Governance through Digital Infrastructure', Government of India, Press Information Bureau, 15 August 2025

Connect with us

Joydeep Ghosh

Partner,
Leader - Life Sciences & Health Care,
Deloitte South Asia
joghosh@deloitte.com

Mayuran Palanisamy

Partner,
Deloitte India
mayuranp@deloitte.com

Pradeep Gupta

Partner,
Deloitte India
pradgupta@deloitte.com

NSN Murty

Partner and Leader,
Government and Public Services,
Technology and Transformation
Deloitte India
nsnmurty@deloitte.com

Vikram Anand

Partner,
Deloitte India
vikramanand@deloitte.com

Alok Saxena

Associate Partner,
Deloitte India
aloksaxena@deloitte.com

Contributors

Ruchika Sareen

Mohd Hussain Shaik

Alankrit Patnaik

Notes

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are approximately 20 lines visible. The paper has a slightly textured appearance.

Notes

[illegible]



Confederation of Indian Industry

No part of this publication may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), in part or full in any manner whatsoever, or translated into any language, without the prior written permission of the copyright owner. CII has made every effort to ensure the accuracy of the information and material presented in this document. Nonetheless, all information, estimates and opinions contained in this publication are subject to change without notice, and do not constitute professional advice in any manner. Neither CII nor any of its office bearers or analysts or employees accept or assume any responsibility or liability in respect of the information provided herein. However, any discrepancy, error, etc. found in this publication may please be brought to the notice of CII for appropriate correction.

Published by Confederation of Indian Industry (CII).

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.