Navigating privacy and protection in India's digital healthcare ecosystem

February 2026

Foreword by PwC

Arnab Basu
Clients & Industries Leader
PwC India

The digital healthcare ecosystem in India is evolving. Health information is among the most important, sensitive, and powerful forms of personal data. It is important to recognise that digital health can advance sustainably only when it is built on the fundamental principles of transparency, accountability, and ethical stewardship. With the growing utilisation of digital technologies in healthcare including AI, algorithms, virtual care platforms and connected medical devices, the responsibility to safeguard patient information becomes more of a moral imperative than a legal obligation.

A privacy-first and security-by-design approach is hence not just an administrative formality—it is the foundation of future-ready healthcare. Strong governance frameworks, clearly articulated consent practices, and resilient mechanisms in cyber defence are essential for building trust in an era where data systems become deeply interconnected and cyber threats more refined. For innovators, suppliers and healthcare providers, it is a call to reconsider operational processes, reinforce ethical guidelines, and incorporate privacy into every workflow—from bedside documentation to cloud-based applications.

As we step into a new era of digital health with the notification of Digital Personal Data Protection (DPDP) Rules, India presents the potential to build an equitable, safe, and citizen-centric healthcare ecosystem. By adopting sensible and accountable practices in data handling, organisations protect the rights of individuals while strengthening the collective resistance of our health systems to malicious exploitations and cybersecurity risks. It is with this belief and responsibility that we should continue our journey towards an empowered, trust-driven, digitally secured, privacy-first future of healthcare in India.

Message from PwC

Dr Rana Mehta
Partner and Leader – Healthcare
PwC India

India's healthcare system is undergoing a swift digitalisation, starting from seamlessly connected health records, telemedicine, remote patient monitoring to AI-enabled clinical decision support systems. This transformation carries potential to strengthen continuity of care, improve work efficiency, expand tertiary healthcare access for rural populations, and deliver many additional benefits. However, as these capabilities scale up, huge volumes of highly sensitive data are being generated, making healthcare systems extremely prone to cyber threats, thereby stressing the need to enhance data privacy and security. The introduction of the DPDP Act, 2023 reinforces this need by defining clear responsibilities for healthcare data fiduciaries, assuring patient rights, and underlining the need for appropriate governance mechanisms.

This report offers a focused view of India's evolving digital healthcare ecosystem, emphasising the risk due to increasing healthtech data production and key privacy challenges, and how regulations such as the DPDP Act can safeguard health data, facilitate innovation, and enhance patient trust.

Message from BCC&I

Angana Guha Roy Chowdhury
Assistant Director General, BCC&I

As we accelerate digital transformation in healthcare with the objective of bringing efficiency, inclusivity, and quality, it is equally imperative to focus on equity, dignity, and data safety.

Health data, coming under the purview of the DPDP Act, 2023, is a central pillar of responsible and ethical healthcare. India has seen rapid adoption of AI, indicating 65% of surveyed Indians are AI users—which is more than double the global average of 31%.[1] Therefore, the need for safeguarding personal data due to the rapid volumes owing to AI, is crucial. There should be an endeavour to leverage the potential of AI rather than succumbing to its vulnerabilities.

As one of the largest generators and processors of sensitive healthcare information—from electronic medical records and diagnostic imaging to telemedicine data and genomics—India's healthcare sector is a priority focus of the DPDP Act and other privacy initiatives.

This makes healthcare service providers (including hospitals, clinics, diagnostic centres), healthtech platforms, and healthcare supply chain players directly liable for the data being generated/processed online or offline. Furthermore, it establishes governance with regulations for transparency, limiting the purpose of data, getting consent, and minimising data.

The process encourages and empowers users to adopt digital healthcare with more confidence. Beyond individual privacy, this also creates the foundation for a responsible, ethical, and transparent healthcare ecosystem backed by robust governance. Investors and regulators are supported in this mechanism to evaluate healthcare facilitators.

The compliance aspect makes the digital framework more robust, building focused security layers and thus safeguarding healthcare service providers against cyberattacks. A robust healthcare ecosystem can have a significant impact on the economy and society, as it is an important aspect which contributes the social and economic resilience of a country.

[1] https://www.ibef.org/news/65-of-indians-used-artificial-intelligence-ai-more-than-double-the-global-average-microsoft-study

Contents

01

Introduction

India has seen an unprecedented increase in the use of digital technologies in the past decade and intends to grow further. According to a 2024 report, India's digital transformation is poised to create a $1 trillion economy by 2028.[2] This includes national digital health initiatives—Ayushman Bharat Digital Mission (ABDM), e-Hospital, eSanjeevani—which were rolled out to improve healthcare accessibility.

[2] https://economictimes.indiatimes.com/news/economy/indicators/india-to-become-1-tn-digital-economy-by-2028-enabled-by-internet-4g-5g-and-digitalisation/articleshow/113875328.cms?from=mdr

Additionally, in the private healthcare sector, there was a sharp rise in electronic medical records, telemedicine platforms, mobile health initiatives—especially due to the COVID-19 pandemic. The rising adoption of AI in healthcare institutions for multiple use cases is leading to large volumes of personal health information being available at a click. While this is leading to better patient experiences and improved operation efficiency, it also raises concerns regarding the appropriate handling of sensitive and confidential patient data.

India's data protection ecosystem has undergone a structured evolution over the years. The recent DPDP Act, 2023—operationalised through DPDP Rules, 2025—enables individuals to have more autonomy over their own personal data. The act also outlines how the data is utilised and processed, with the Data Protection Board of India acting as the enforcement body. All the entities processing digital personal data must adhere to the obligations of the DPDP Rules by 13 May 2027 (i.e. within 18 months of the notification in November 2025).

It is important to note that the timeline is compressed for a sector that has seen limited adoption of digital tools, despite the recent digital growth, as compared to other sectors. However, on the other hand, this poses an opportunity to embed privacy aspects at the development stage itself, making it easier than adding these controls in existing systems. Within healthcare, ABDM is a considerable example of security by design or privacy-first due to its federated data architecture, along with a consent manager for health information exchange for secure interoperability.[3]

Against this backdrop, it becomes crucial to understand how hospital leadership perceives their organisation's awareness, readiness, and capacity to implement the DPDP requirements.

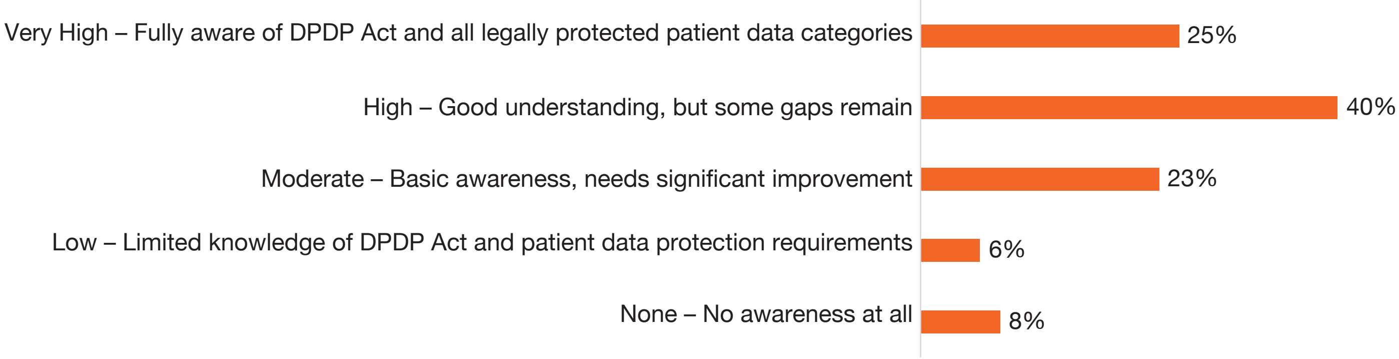
In January 2026, PwC India surveyed healthcare professionals to capture the industry sentiment about the evolving digital data privacy and protection regulations and their impact on the digital healthcare landscape. The survey received a fair mix of responses from an array of respondents across different roles—with about 40% responses from CXOs/directors/business unit heads, and the rest from healthcare administrators and professionals.

From an institutional standpoint, 65% respondents were from sizeable healthcare facilities with over 300 beds. This was followed by 25% respondents comprising healthtech providers and diagnostics, and just over 10% respondents belonging to medium and small healthcare facilities and insurance providers.

As a starting point, the first question aimed to understand the current level of awareness of digital data protection duties. Almost 65% of the respondents felt they were aware of the requirements, while rest indicated they had limited understanding, highlighting gaps which could have an impact on the overall readiness and compliance with the requirements. Even though more than 50% of the responses indicated a good level of understanding of the requirements, it remains to be seen whether this understanding is adequately reflected in the actions taken by organisations in their journey towards achieving compliance.

Figure 1: Organisation's familiarity with the DPDP Act, 2023

How would you rate your organisation's familiarity with the Digital Personal Data Protection (DPDP) Act, 2023, and its understanding of which patient data categories require extra legal protection?



[3] https://abdm.gov.in/static/media/Session%206%20-%20Digital%20health%20-%20Privacy%20&%20Security.083a5b3e73ba533e321b.pdf

This graph highlights different levels of familiarity with the DPDP Act among organisations and the importance of navigating India’s expanding digital healthcare sector. With only 25% fully aware of the DPDP Act and all of them being legally protected patient data categories, many organisations may struggle to align with the Act’s obligations. 40% respondents possess a high yet incomplete understanding of certain aspects of the act, which suggests room for improvement and a need for education to ensure compliance. 23% respondents with moderate awareness and the remaining with low or no knowledge highlights significant gaps, posing risks in safeguarding patient data as digital healthcare infrastructure becomes more integral to healthcare delivery in India. Addressing these educational gaps is crucial to secure and resilient growth.

02 India’s digital healthcare landscape

The healthcare sector in India, which is historically characterised by fragmented delivery models, uneven access, and paper-based records, is now moving towards a more connected, interoperable, and data-centric ecosystem. The system is undergoing a structural transformation driven by rapid digitisation, policy reform, and the expansion of digital infrastructure in the public domain. As we continue to address the challenges of 2026, the convergence of universal digital identities, stringent laws of data protection, and advanced medical technologies has redefined the patient–provider relationship. This evolution is no longer limited to creation of digital records—it is about forming a secure, interoperable, and predictive health economy that serves nearly 1.5 billion people. This development has been accelerated by rising healthcare demand, increased smartphone and internet penetration, and strong government leadership in establishing digital platforms at a population scale.[4]

[4] India Brand Equity Foundation (IBEF). (2024). Healthcare Industry in India. Sourced from https://www.ibef.org/industry/healthcare-india

The foundation of this transformation remains ABDM (previously National Digital Health Mission). Since its inception, the mission has scaled rapidly, moving from a pilot framework to become the national backbone for health data exchange. Currently, the issuance of over 84.8 crore ABHA IDs and the linking of more than 82.7 crore health records have created a longitudinal health database for a vast majority of the population.[5] With ABHA IDs compromising sensitive personal data, the introduction of the DPDP Act is both timely and strategic, ensuring well-aligned protection for the rapidly growing volumes of digitised healthcare information. The infrastructure allows for the seamless flow of data between primary care centres and tertiary hospitals, regardless of location. The recent integration of AI-driven multilingual translation tools like Bhashini into the ABDM ecosystem will further democratise access, ensuring that patients can interact with digital platforms in their native languages, thereby bridging the deep-rooted digital divide between the rural and urban population.

Parallel to this growth is the exponential adoption of telemedicine and digital pharmacies. What began as a necessity during the pandemic has matured into a multi-billion-dollar industry, with Indian telehealth market size being projected to reach $11.39 billion by 2031, growing at a CAGR of 19.71% from 2026 to 2031.[7] Telemedicine is no longer used as a secondary option—it is now primarily used for chronic disease management and mental health support. Platforms like eSanjeevani have proven the influence of the public sector in the digital health ecosystem by delivering hundreds of millions of consultations, while e-pharmacies are projected to capture nearly 10% of total pharmaceutical sales.[8] These digital pharmacies are increasingly supporting e-prescriptions to confirm medication continuity and preventing the misuse of drugs, creating a closed-loop system that increases patient safety.

The current digital health technology landscape is also defined by the rise of AI in clinical adoption and remote patient monitoring. In 2026, medical-grade wearables have evolved from lifestyle gadgets into critical clinical tools that provide real-time data on glucose levels, cardiac rhythms, and respiratory health.

This swell of data is processed through AI algorithms assisting clinicians in predictive diagnosis, reducing the burden on an already strained healthcare workforce. The predominant segment in the current digital health market is digital fitness and wellbeing which has evolved from lifestyle tracking to a major tool for disease management and providing prescriptions for conditions ranging from diabetes to clinical depression. The innovation engine fuelling this digitisation is also largely maintained by a dynamic ecosystem of healthcare startups who are increasingly focusing on specialised areas as AI-assisted radiology, cold chain logistics, and AI chatbots in care management, ensuring that the benefits of the digital frontier reach the last mile. However, as these tools depend largely on the continuous collection and processing of high-resolution patient data, the integrity and security of this data becomes a major concern.

This rapid digitisation is occurring within a new and careful regulatory environment defined by the DPDP Act. In 2026, privacy is no longer an afterthought but a core design requirement. Healthcare providers, categorised as data fiduciaries, must operate under a 'consent-first' architecture, where every digital interaction is preceded by explicit, itemised consent.

For large hospital chains and healthtech providers designated as significant data fiduciaries, the concerns are larger—including mandatory audits and appointment of dedicated data protection officers to evade the risk of substantial business penalties.

The legal framework has forced the industry to move towards a 'privacy-by-design' approach ensuring data protection is guaranteed in the development of the digital health ecosystem. In addition to this, the newly introduced DPDP Rules emphasise that use of algorithms in AI models must be reviewed periodically, to ensure that fiduciaries do not deny an individual's right to privacy due to archaic or biased systems. By mandating continuous oversight, the rules emphasise on accountability and safeguarding against risks that emerge when legacy models are left unchecked in acute healthcare decision-making scenarios.

However, DPDP Rules 2025 provide definite exemptions to this consent-first model, granting data processing without prior consent in closely defined contexts as in medical emergencies (Rule 7) and research or statistical purposes (Rule 8), provided safeguards against re-identification are maintained. These exemptions highlight the balance between safeguarding personal privacy and enabling critical healthcare and research functions.

As we move forward, the acceleration of digitisation in Indian healthcare is inevitable. The challenge in the upcoming years will lie in keeping the right balance through rapid innovation and the fundamental right to data privacy. In the digital frontier, trust has become a leading currency and ensuring protection of the patient data will help India truly realise the potential of this healthcare revolution.

[5] National Health Authority (2026). ABDM Public Dashboard: Real-time statistics on ABHA Ids and Health records. Government of India, Ministry of Health & Family Welfare. https://dashboard.abdm.gov.in/abdm/

[6] Press Information Bureau. (2026, January 19). Signing of Memorandum of Understanding (MoU) between Digital India BHASHINI Division and National Health Authority. (Release ID: 2216227)

[7] Mordor Intelligence (2026). India Telehealth Market Size & Share Analysis. Sourced from https://www.mordorintelligence.com/industry-reports/telehealth-services-market-in-india

[8] Mordor Intelligence (2026). India Pharmaceuticals Market Size & Share Analysis. Sourced from https://www.mordorintelligence.com/industry-reports/pharmaceuticals-industry-in-india

03 Healthcare and privacy regulations

3.1 The evolution of privacy laws: How GDPR and the DPDP Act are shaping a new digital world

Protecting patient privacy is essential not just for legal compliance, but for ethical and clinical integrity in healthcare systems. Regulations such as the General Data Protection Regulation (GDPR) in the EU and DPDP Act, 2023 and DPDP Rules, 2025 in India create a structured legal foundation that governs the handling of personal heath data—an inherently sensitive category of information.

Understanding the perceived core objectives of these regulations, especially the DPDP Act in the healthcare sector, is crucial for effective implementation and adherence. Industry perspectives reveal a strong consensus on the primary goal:

Figure 2: Primary purpose of DPDP Act in healthcare

How would you describe the primary purpose of the DPDP Act in healthcare?

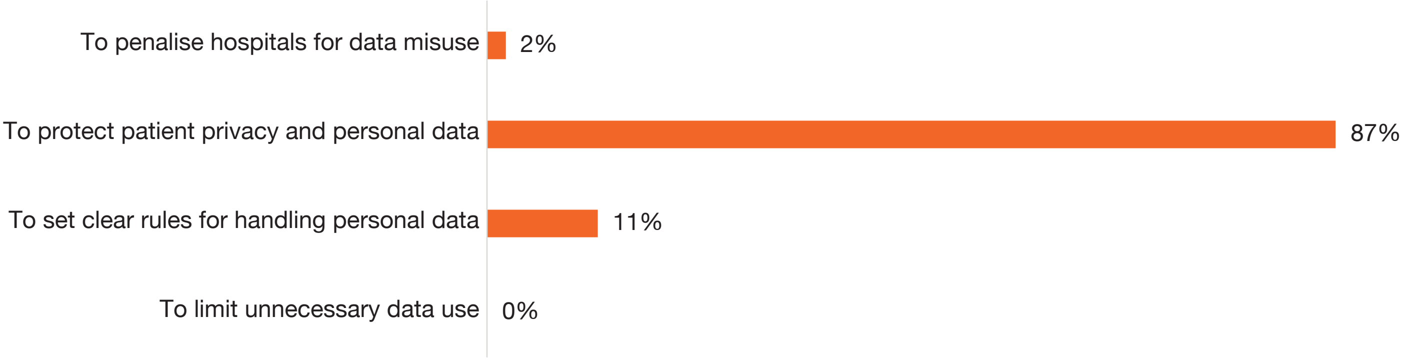


Figure 2 highlights the perceptions of the DPDP Act's primary purpose in healthcare. Majority of the respondents (87%) view the regulation as a means to protect patient privacy and personal data, thus enabling trust and security in healthcare. 11% of the respondents emphasised the need for clear rules for handling data—for example, establishing clear standard operating procedures. Only 2% see it as a tool for penalising data misuse, suggesting that the focus is more on proactive protection than as a medium to avoid penalties, which is a positive step in the compliance journey.

The findings reflect positive stakeholder mindset in support of a privacy-first approach. This understanding of the DPDP Rules to enable and protect privacy, establishes its social acceptance at large.

The DPDP Act and DPDP Rules frameworks highlight several key benefits:

3.1.1 Protect patient autonomy by giving individuals control over access, sharing, and secondary use of health data.

3.1.2 Strengthen trust in digital healthcare systems, improving patient disclosure and care outcomes.

3.1.3 Mandate governance mechanisms such as Data Protection Impact Assessments (DPIAs), breach reporting, and accountability frameworks.

3.1.4 Reduce cybersecurity risks through compulsory safeguards (encryption, access controls, audits).

3.1.5 Enable ethical research and innovation via anonymisation and lawful secondary use of health data.

3.1.6 Align domestic healthcare systems with global privacy standards, supporting cross-border care and research.

3.2 Child healthcare exemptions

Specific to the healthcare sector, the DPDP Rules, 2025, acknowledge the unique requirements of child health data. They provide specific exemptions from general consent requirements (sub-sections [1] and [3] of Section 9 of the act) for certain healthcare entities and purposes, ensuring child welfare without impeding essential care or safety. These include:

Exempted healthcare entities (Fourth Schedule Part A):

- **Clinical establishments, mental health establishments, and healthcare professionals:** Processing is restricted to providing health services to the child, to the extent necessary for their health protection.
- **Allied healthcare professionals:** Processing is limited to supporting the implementation of recommended healthcare treatment or referral plans for the child's health protection.
- **Educational institutions (including vocational education):** Processing is restricted to tracking and behavioural monitoring for educational activities or for the safety of the enrolled children.
- **Crèches or child daycare centres:** Processing is confined to tracking and behavioural monitoring for the safety of the children entrusted to the daycare facility.
- **Entities engaged for child transport:** Processing is restricted to tracking the child's location in the interest of their safety, during travel to and from the institution, crèche, or centre.

Exempted purposes for child data (Fourth Schedule Part B):

- Exercising any legal power, function, or duty in the child's interest
- Providing subsidies, benefits, services, certificates, licences, or permits to the child
- Creating user accounts for email communication (limited to email only)
- Determining real-time location for the child's safety and protection
- Ensuring the child is not exposed to harmful information, services, or advertisements
- Processing for the purpose of confirming that a data principal is not a child and performing due diligence as per Rule 10

3.3 Case studies: Disclosure of employee data without their consent

3.3.1 Disclosure of an employee's special category data by their employer to a third-party services provider, without the employee's consent[9]

- **Background**

An employee submitted a data access request to their employer—a small and medium enterprise B2B service provider. Based on the documents received, the employee discovered that their personal data—including medical and health-related information (special category data)—had been disclosed to a third-party HR service provider without their explicit consent.

- **Key issue**

The employer shared extensive personal and medical data with an external HR provider as part of an internal bullying investigation, despite the employee having explicitly requested that their data not be disclosed to third parties.

- **Data Protection Commission (DPC), Ireland assessment**

  The DPC examined whether:

  - A valid lawful basis existed under Article 6 GDPR
  - A lawful condition for processing special category data existed under Article 9 GDPR
  - The data shared was necessary and proportionate, in line with data minimisation

[9] https://dataprotection.ie/en/dpc-guidance/case-studies/disclosure-unauthorised-disclosure/disclosure-employees-special-category-data-their-employer-third-party-services-provider-without

- **Findings**
  - The organisation failed to clearly identify and document the lawful basis (e.g. consent, contract, legal obligation, vital interests, public task, or legitimate interests) relied upon for the disclosure.
  - No evidence was provided of a legitimate interest assessment prior to disclosure.
  - The disclosure of medical data lacked a valid Article 9 condition.
  - The volume and nature of data shared were found to be excessive.
- **Key takeaways**
  - Special category data requires explicit legal justification, not just assumptions.
  - Third-party disclosures must meet necessity and proportionality tests.
  - Lawful basis decisions must be clearly documented and defensible.
  - Employee data in investigations needs heightened privacy safeguards.

3.3.2 Excessive sharing of special category data to a third party to seek guidance on behalf of an employee[10]

- **Background**

A public sector employee shared medical documents with the organisation's disability officer to seek reasonable workplace accommodation. During discussions, the employee also disclosed personal health, financial, and family information. The disability officer subsequently shared extensive personal and health data with a third-party employee assistance service without the employee's consent, leading to concerns about excessive and unexpected data disclosure.

- **Core issue**

Whether the organisation could lawfully share special category data with a third party under the GDPR, and whether the amount and nature of data shared were necessary and proportionate for the purpose claimed.

[10] https://dataprotection.ie/en/dpc-guidance/case-studies/disclosure-unauthorised-disclosure/excessive-sharing-special-category-data-third-party-order-seek-guidance-behalf-employee

- **DPC's assessment**

  The DPC reviewed whether:

  - The purpose was legitimate and compatible.
  - The data shared was limited to what was needed.
  - The legal basis cited was applicable in the circumstances.

- **Findings**

  - The amount of personal data shared was excessive relative to the purpose.
  - Use of vital interests' legal basis was invalid because that basis applies only to immediate, life-threatening situations—no such situation existed here.
  - The organisation acknowledged that an anonymised description could have achieved the same purpose without sharing identifiable personal or health data.
  - No evidence showed the employee had been informed their data could be shared with third parties for guidance at the time of disclosure.
  - As a result, the processing was not compliant with GDPR principles on purpose, necessity, and transparency.

- **Key takeaways**

  - Lawful basis is mandatory for third-party sharing, especially for special category data.
  - Data subject expectations must be considered before any further use of data.
  - Minimise disclosures by using anonymised summaries wherever possible.
  - Be transparent upfront about any potential third-party data sharing.

3.4 Existing digital regulations in healthcare

3.4.1 Information Technology Act, 2000 & IT Rules (SPDI Rules, 2011)

It covers cybersecurity and data protection, security practices, and protection of Sensitive Personal Data or Information (SPDI). This act applies to health data until DPDP Rules are fully operational.

3.4.2 DPDP Act, 2023

This act covers protection of personal and sensitive digital data, explicit consent for data processing, data minimisation and purpose limitation, and data breach notification. It applies to electronic medical records (EMRs), hospital information systems (HIS), health data classified as sensitive personal data, hospitals represented as data fiduciaries.

3.4.3 CERT-In Directions, 2022 (Cybersecurity Incident Reporting)

This is a mandatory operational regulation applicable to hospital IT infrastructure. It mandates reporting cyber incidents within six hours of occurrence.

3.5 Key provisions for consideration

3.5.1 The DPDP Act, 2023, along with DPDP Rules, 2025, outlines a framework for the protection of personal data processed in India.

As healthcare organisations are known to process sensitive personal data such as medical history and records regularly through various platforms, several sections of the act and rules require special attention from a healthcare perspective. These provisions impose stricter obligations on healthcare data fiduciaries while also accounting for the realities of care delivery through exemptions.

3.5.2 Classification of healthcare entities as data fiduciaries

Healthcare service providers, such as hospitals, clinics, diagnostic centres, health technology platforms, telemedicine services, and HIS suppliers, have been classified as data fiduciaries under the act. This classification makes the entities responsible for the lawful processing, protection, and governance of personal and sensitive data in the healthcare sector. Being highly sensitive in nature, health data is a subset of sensitive personal data that requires high levels of protection and strict purpose limitation.

3.5.3 Consent-centric processing with sector-specific flexibilities

The DPDP Act provides free, informed, specific, and unambiguous consent as the default ground for processing personal data of individuals. In the healthcare sector, this applies to activities such as patient registration, diagnosis, teleconsultation, insurance processing, digital health applications, and interoperable health information exchange. However, the act recognises that consent may not always be possible in the healthcare sector. Processing without consent is allowed if it is required in medical emergencies, life-threatening situations, or public health interventions as authorised by the state.

3.5.4 Purpose limitation, data minimisation, and retention in healthcare operations

Healthcare data fiduciaries are required to collect and process the personal data that is necessary for specific purposes. The rules detail the requirements for the deletion of personal data after the purpose of processing has been achieved, except when retention is required by applicable medical, legal, and regulatory requirements. Further, in the healthcare industry, there is a need for a balance between the rights of patients and the requirements of clinical continuity and medico-legal record-keeping. Retention schedules and communication with patients are important for the same.

3.5.5 Security safeguards and breach management obligations

The DPDP Rules mandate the implementation of reasonable technical and organisational measures to avoid personal data breaches. For the healthcare sector, this would include encrypting healthcare records, implementing role-based access controls, masking and tokenisation of sensitive identifiers, continuous system monitoring, and secure backup processes. These measures are required to be extended to third-party data processors through contractual agreements.

In the case of a personal data breach, healthcare data fiduciaries are required to notify the affected individuals and the Data Protection Board of India, specifying the nature of the breach, its potential impact, and remedial measures. With respect to the critical nature of healthcare services, breach preparedness, and response planning take on added significance.

3.5.6 Enhanced obligations for significant data fiduciaries in healthcare

Hospital chains, diagnostic centres, and digital health platforms that handle large amounts of personal data may be classified as significant data fiduciaries. They have additional obligations, such as appointing a data protection officer, performing periodic DPIAs, independent auditing, and enhanced oversight of algorithmic and AI systems. These obligations hold a special significance as the healthcare sector is increasingly adopting AI for diagnostic, remote monitoring, and predictive purposes.

3.5.7 Permitted use of health data for research and statistical purposes

Within the DPDP Act, personal data can be processed for research, archival, and statistical purposes under some specific conditions. In the healthcare industry, this allows clinical research, public health research, and innovation—as long as the processing is lawful, proportional, secure, and in line with the established standards. Anonymisation and de-identification are important tools that make the above possible without compromising re-identification.

3.5.8 Digital-first regulatory and grievance redressal mechanisms

The DPDP Rules mandate that the Data Protection Board of India and the appellate tribunals allow for electronic filing, hearings, and grievance redressals. This is in line with the digital governance structure in the healthcare industry, ensuring easy compliance and redressal without interfering with the important healthcare functions.

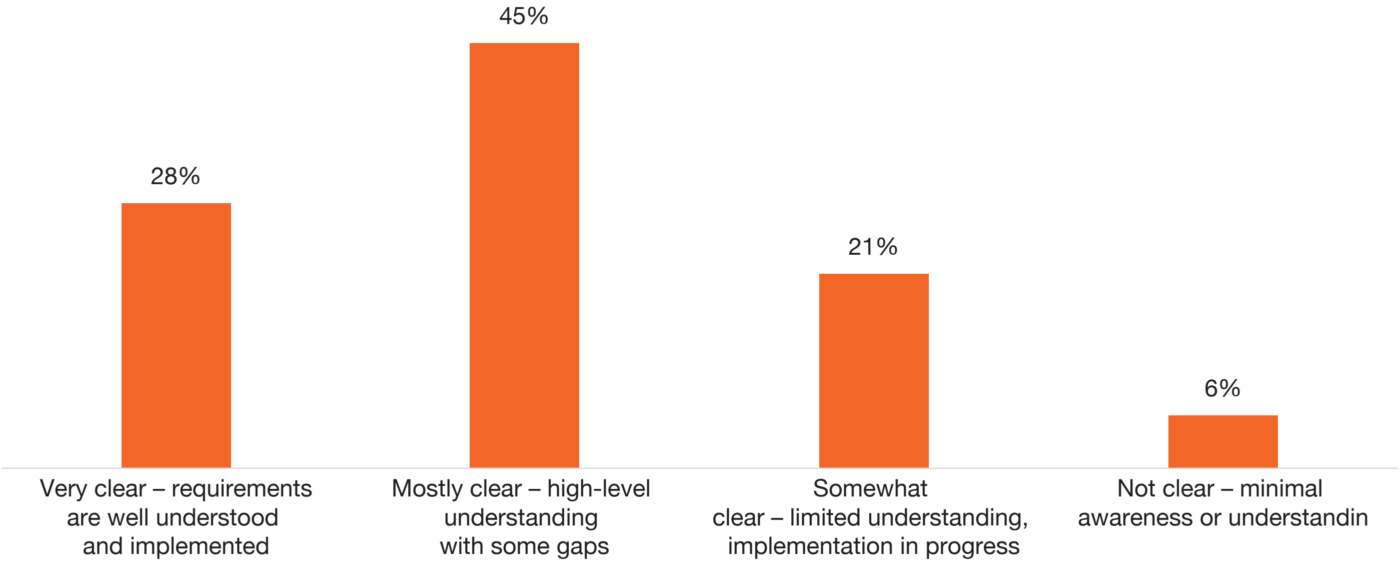
04 Privacy challenges due to the digitisation of the healthcare sector

The digital transformation in the healthcare industry has significantly expanded volume, variety, and velocity of personal health data. While this shift has improved care delivery, research-driven innovation, and operational efficiency, it has also introduced complex privacy risks arising from data proliferation, opaque data flows, long data lifecycles, and multi-party ecosystems. Addressing these challenges requires a nuanced understanding of both technological as well as governance limitations across modern healthcare systems.

One of the key considerations in overcoming governance limitations and ensuring effective data protection is the organisational clarity and preparedness regarding the key data protection regulations. However, as recent survey findings indicate, there can be significant variance in this understanding across healthcare entities, which poses its own set of challenges.

Figure 3: Understanding of the DPDP Act and its applicability

How clear is your understanding of the requirements of the Digital Personal Data Protection Act (DPDPA) as applicable to your healthcare organisation?



While 73% of the respondents feel their understanding is clear about the requirements and 28% indicated complete implementation, the figures suggest a possible perception gap instead of actual readiness. Furthermore, 21% of the respondents highlighted having a limited understanding, and 6% admit they are barely aware about the requirements of the DPDP Act.

4.1 Expanding digital footprints and exposure

Digital healthcare now extends beyond the traditional clinical records to include information from mobile apps, wearables, IoT devices, and digital platforms. When this information is combined with medical records, even seemingly non-clinical data becomes sensitive, thus significantly increasing the risks of re-identification, profiling, and misuse across interconnected systems.

4.2 The hidden risks of reduced patient awareness

Patients often have limited visibility into how their health data is being gathered, shared, and reused across digital ecosystems. Complex consent mechanisms and consent fatigue often reduce meaningful understanding, weaken informed decision-making, and undermine trust in digital healthcare services.

4.3 Data persistence and secondary use risks

Health data are inherently long-lived and may be retained beyond their primary purpose. Secondary use—analytics, research, or AI development—raises concerns around purpose limitation. At the same time, studies show that anonymisation alone does not fully eliminate re-identification risks when datasets are combined.

4.4 Governance and operational weaknesses

Many healthcare organisations face governance issues due to several challenges such as inconsistent privacy audits, fragmented legacy systems and uneven enforcement of safeguards. These challenges are further amplified by complex third-party ecosystems, where limited oversight increases vendor-related privacy and security risks.

4.5 Ethical tension: Privacy vs innovation

Healthcare digitalisation raises an inherent tension between protecting patient privacy and enabling innovation. Overly restrictive approaches can slow medical research and AI adoption, while insufficient safeguards can risk data exploitation and erosion of public trust, highlighting the need for context-sensitive governance models.

While large healthcare organisations with strong digital capabilities are making good progress, many smaller or less digitally advanced providers are still far from full compliance. The 18-month timeline is ambitious, especially considering the wide range of sizes and digital maturity across healthcare providers. Integrating privacy by design principles with digital health initiatives is viewed as the best way to make implementation achievable, as building in privacy from the start helps ensure seamless compliance. However, given the current pace and the complexity of the task, it is likely that the sector may request extensions or phased implementation—particularly for smaller organisations or more complicated areas of compliance.

05

Security, risk, and protective measures

Protecting health data demands not just compliance with regulatory mandates but also a proactive, risk-based security posture embedded across people, processes, and technology. Because of the sensitivity, longevity, and criticality of healthcare data, organisations need to adapt layered security controls, strong governance mechanisms, and resilience-focused practices to prevent, detect, as well as respond to the risks arising because of cyber and privacy attacks.

5.1 Privacy by design and risk governance

Effective protection of health data begins with the integration of privacy into system design rather than adding controls later. Risk assessments, DPIAs, and clearly defined accountability roles such as data protection officers or chief privacy officers form the foundation of sustainable and compliant healthcare data governance.

5.2 Technical security safeguards

Healthcare systems require multi-layered technical controls, which includes, but is not limited to, encryption, strong authentication, and role-based access management. Continuous monitoring is necessary to detect unauthorised access as early as possible and to reduce the likelihood and impact of data breaches which involve sensitive health information.

5.3 Incident response and resilience

Given the frequency and severity of healthcare cyber incidents, organisations must maintain effective incident response and breach management plans. Early detection, containment, and notification processes are necessary in order to limit harm and maintain regulatory and stakeholders' trust.

5.4 Organisational and cultural controls

Security and privacy controls are effective when supported by organisational culture. Regular staff training, internal audits, and leadership involvement play a critical role in lowering human error, strengthening accountability, and embedding privacy-aware behaviour across various healthcare operations.

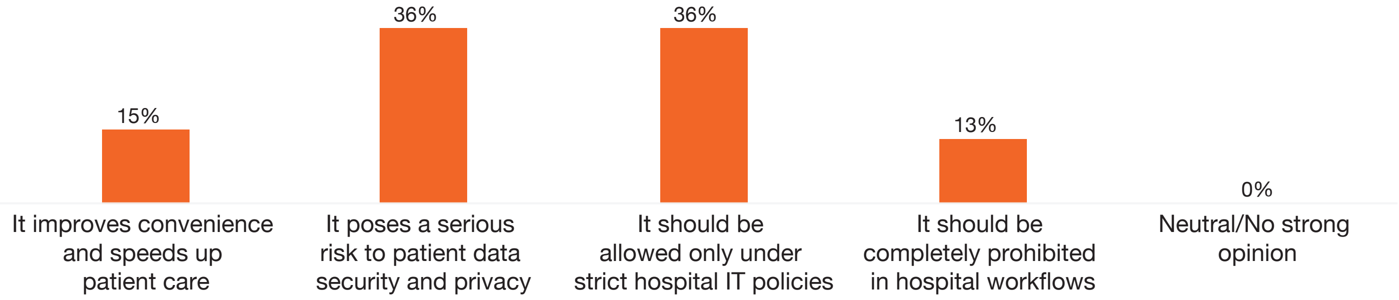
5.5 Third-party and ecosystem risk management

Healthcare data environment is becoming more reliant on third-party vendors, platforms, and service providers, thus increasing the overall risk exposure. Effective contractual safeguards, technical controls, and continuous monitoring are thus necessary to prevent downstream privacy failure originating outside the core organisation.

Despite the presence of robust frameworks and controls, the evolving digital landscape introduces new complexities—especially in areas where personal technology and professional practice interact. The proliferation of personal devices and consumer-grade communication platforms presents a unique dilemma for healthcare organisations striving to balance operational efficiency with stringent data security and privacy mandates. This tension is clearly reflected in the recent industry perspectives on staff practices, as illustrated below:

Figure 4: Use of personal devices to share health data

What are your thoughts on hospital staff using personal devices (e.g., email, WhatsApp) to share patient reports and access lab results?



There was a split between two groups of respondents: 36% of the respondents view it as a serious security and privacy risk and another 36% believe it should be allowed only under strict IT policies. A smaller group (15%) views it as a convenience that speeds up care, and about 13% of the respondents feel it should be completely prohibited.

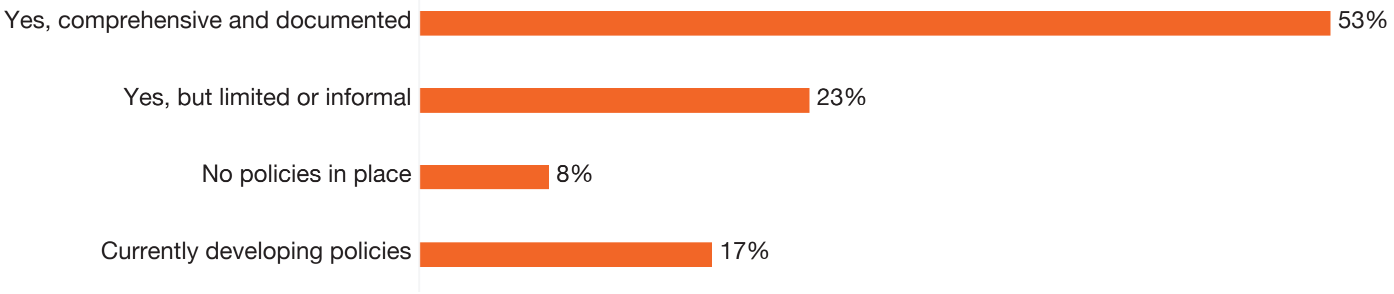
With the increase in digital care, practices of bring your own device without controls exposes the ecosystem to risks of data leakages and weak audit trails. Policy-bound use of patient data, aligned with the requirements of the DPDP Rules, can provide the requisite guardrails to mitigate these risks.

06 Technology enablers for protection and privacy

The DPDP Rules, 2025 significantly strengthen India's data privacy regime by requiring safeguards like encryption, tokenisation, and restrictive limits on access, aligning domestic process with worldwide standards. By tightening privacy and consent requirements—including parental consent and more strict data handling—the rules promote a transparent, privacy-first digital space that safeguards individuals and holds organisations accountable. This is very crucial for healthcare, where rapid digitisation demands formal protection policies and having clear awareness of the risks to health data in India.

Figure 5: Data protection policies

Does your hospital have formal data protection policies in place?



PwC's survey shows that just over half of the respondents (53%) report they have implemented exhaustive, well-documented data protection policies, showing improvement in privacy governance. However, 23% depend on basic or informal measures, 17% are still developing formal policies, and 8% have no policies—pointing to major gaps despite national efforts to enhance privacy standards in healthcare.

Documented policies convert the principles of DPDP into day-to-day operational practice. While half of the hospitals self-report as being policy-ready, the rest need to find gaps in their digital programs and systemise their standards to ensure operational safeguards.

6.1 Key threats to data protection and privacy in India

- **Cyberthreats and data breaches:** Hospitals and health technology platforms are primary targets for cybercriminals, owing to the high value of medical data on illegal markets.
- **Ransomware attacks:** File encryption attacks can severely interrupt healthcare operations by encrypting essential systems, often forcing organisations to pay a ransom or risk interrupting crucial provisions, including critical care.
- **Phishing and social engineering:** Healthcare personnel are commonly targeted by phishing and social engineering schemes that exploit human security weakness that allow unapproved system access.[11]
- **Insider threats:** Individuals within the organisation, team members, or contracted individuals who have approved access may deliberately or inadvertently compromise sensitive health information—a risk that is heightened when obsolete systems lacking proper protective measures or the use of tools like Excel bypass essential HIS safeguards such as audit logs, access permission, data encryption, and security policies.
- **Credential stuffing and password attacks:** Cyber attackers commonly use stolen or recycled credentials to penetrate systems through methods like automated credential login attempts and password attacks.
- **Obsolete systems and legacy applications:** Disused or unsupported systems may lack critical security patches and modern safeguards, leaving sensitive health data exposed to potential misuse.
- **Use of non-secure data handling practices:** Reliance on spreadsheets or manual Excel files instead of a centralised HIS potentially exposes data to unauthorised access, accidental leakage, and poor auditability.
- **Siloed data governance:** Storing patient information across fragmented, non-integrated tools can increase the risk of inconsistent data practices, ineffective access control enforcement, and difficulty in enforcing compliance with data protection standards.
- **Limited monitoring and audit trails:** Legacy platforms and ad-hoc storage often lack robust logging and monitoring capabilities, reducing the ability to detect issues, making it harder to quickly spot unusual activity, misuse by insiders, or external attacks.

[11] https://www.digitalhealthnews.com/health-data-privacy-india

6.2 Key technology enabler for privacy and security in healthcare

- Privacy-enhancing technologies (PETs) let organisations securely access, share, and analyse private data without exposing personal information. They lower privacy risk, strengthen compliance with GDPR and Health Insurance Portability and Accountability Act (HIPAA), and enable responsible AI in high-risk sectors like healthcare, banking, and government.
- PETs unlock siloed datasets by supporting safe aggregate health insights (e.g. disease incidence, vaccination trends) without exposing personal records. Methods like such as federated learning allow hospitals to collaboratively train models for disease prediction or patient-risk scoring without moving raw clinical data; secure multi-party computation enables joint review of encrypted datasets to assess measure the treatment outcomes; and fully homomorphic encryption allows data to remain encrypted while still enabling meaningful computations on it, ensuring privacy throughout processing.[12]
- In India, the government is preparing to scale PETs under the DPDP Act, with Ministry of Electronics and Information Technology indicating priorities around federated learning, formal privacy, and homomorphic encryption—paired with developer training and PET-based architectures across large public systems—positioning India to lead in privacy-preserving digital governance.[13]

6.3 Key standard practices for compliance management

- **Consent and processing management:** DPDP solutions enable organisations to capture clear, revocable consent and link processing to specific purposes, automatically stopping data use if consent is withdrawn to ensure compliance.
- **Data principal rights and security:** They automate handling of rights requests (access, correction, erasure, portability) within mandated timelines and keep track of audit logs. The platforms also map data, assess risks, and apply strong security like encryption and role-based permission.
- **Regulatory monitoring and reporting:** With real-time dashboards, these platforms track consent, rights queries, and processing compliance. They generate audit-ready reports and oversee third-party processor adherence to DPDP rules.

Despite progress in privacy guidelines framework and policy oversight, many organisations are still developing data protection capabilities. Leading DPDP compliance platforms help enforce consent, rights, and monitoring, strengthening safety and trust. Overall, India is building a strong, robust platform for secure digital health, though wider adoption and continuous monitoring remain essential.

[12] https://www2.itif.org/2025-pets-tech-explainer.pdf

[13] https://www.medianama.com/2025/11/223-privacy-enhancing-technologies-pet-dpdp-meity/

07 Stakeholder collaboration for a privacy-first healthcare ecosystem

The previous sections highlight the new obligatory regulations, descriptive case studies and various safeguards that need to be in place in order to ensure safety of sensitive patient data. However, just setting controls is not enough. Actual compliance lies in the collective alignment of all stakeholders accountable for creating, accessing, processing and managing health data.[14]

[14] https://abdm.gov.in/static/media/Session%206%20-%20Digital%20health%20-%20Privacy%20&%20Security.083a5b3e73ba533e321b.pdf

A single organisation—be it a hospital, healthtech platform, diagnostic chain, clinic—cannot achieve a privacy-first ecosystem as an isolated entity. Healthcare data moves across platforms from laboratories to hospitals to payers, and at each of these, the risk of a breach is present with the possibility of exposure in the absence of appropriate safeguards and practices. Safe health information exchange requires a shared responsibility between all stakeholders to ensure appropriate action and responsibility is taken up across the value chain to create a secure healthcare system.[15]

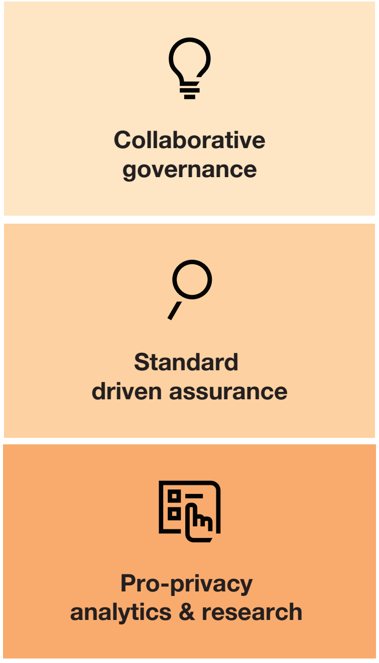
To address this, there is a need to adopt more collaborative governance models across internal and external stakeholders including healthcare providers, technology vendors, third party administrators, payers, diagnostic centres, pharmaceuticals, and digital health platforms to understand obligations and alignment with the requirements at every step because even a single weak link can put the entire ecosystem at risk.

a. **Collaborative governance:** The DPDP Act, 2023 and DPDP Rules, 2025 do not directly mandate a governance structure. They only explicitly mention:
   - Accountability for outcomes
   - Establishing steering committees or councils with representatives from respective entities to drive unified policy development
   - Data-sharing agreements with service-level expectations for privacy and security
   - Clear contractual clauses
   - Alignment on interpretation of compliance requirements
   - Identification of major risks
   - Creation of strong breach response processes to ensure a reliable mechanism to distribute responsibility and support safe sharing and protection of sensitive patient data

b. **Standards-driven assurance and consent verification:** Incorporate standardised data formats and exchange protocols to enable secure flow of data between decentralised systems to ensure every transfer is purpose-bound, logged, time-limited, auditable, and processed only after verifying the patient's authorisation to access their health records.

c. **Pro-privacy analytics and research:** The DPDP Act and Rules aim to safeguard personal data through a data protection board of India. This will be done while aligning with the Draft National Data Governance Framework Policy[16] which ensures that non-personal and anonymised data from both government and private entities will be safely accessible for research and innovation through India Data Management Office. As clinical insights, health analytics, and AI in healthcare continue growing and with the government promoting these innovations,[17] requirement for safe use of health data for research is of utmost importance. Furthermore, de-identification of data is essential as this will allow research to continue while upholding individual privacy.

Figure 6: Synergy mechanisms



Though alignment across entities is important, it is equally essential to have internal stakeholder alignment. Data privacy does not solely sit within IT/compliance functions. Clinical teams, administrators, clinical and non-clinical managers, and other staff should be able to understand how their day-to-day activities involve interaction with patient data and what is expected of them to safeguard the data. An Organisation for Economic Co-operation and Development (OECD) report[18] stresses on running regular training programmes on patient data sensitivity, consent rules, breach escalation, and safe data-sharing practices to help teams understand their roles and move towards a privacy-aware culture that balances compliance and care delivery.

The transition to a privacy-first culture is not a mere compliance activity; it needs to be a joint responsibility to build trust where each member demonstrates the commitment to protecting patient data with consistency.

[15] https://www.oecd.org/en/publications/health-data-governance-for-the-digital-age_68b60796-en.html

[16] https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf

[17] https://www.digitalhealthnews.com/pm-modi-calls-on-indian-ai-startups-to-prioritize-healthcare-innovations

[18] https://www.oecd.org/en/publications/health-data-governance-for-the-digital-age_68b60796-en.html

08 Healthcare in balance: Harmonising care and compliance

Quality patient care and compliance requirements are sometimes brought up as distinct priorities in medical institutions. They collide every day—on hospital floors, in clinical decision-making, and in leadership meetings. The most essential task for healthcare leaders is thus ensuring that not only are these aspects given equal importance but they are also complementing each other in a seamless manner, without obstructing the other. Companies that handle this equilibrium effectively usually view it more as a cultural and operational problem than just a legal one. They understand how good results, moral behaviour, and discipline for compliance are closely related.

Outcomes and experience, not catchphrases, help us to best appreciate good patient care. Good patient care can be defined by fewer avoidable mistakes, better care transitions, more effective communication, and patients who feel respected instead of hurried. Leading companies see quality as a continuous responsibility rather than a fixed standard. Good quality in today's world is also closely related to public trust, since patient feedback and performance data are more readily available than ever.

8.1 Understanding healthcare compliance

Healthcare compliance is often mistaken as a peripheral legal requirement. In reality, it functions as a framework that enables moral and safe delivery of care in a highly regulated setting. To lower variation and safeguard patients as well as institutions, rules and laws controlling privacy, billing methods, patient safety, and professional behaviour are in place. For instance, US rules like HIPAA were created to protect patient information while also outlining organisational duties with regard to data handling and disclosure.[19] Tension usually results from the perception of disconnection between clinical reality and compliance rules. Time spent on direct patient care can conflict with paperwork needs, reporting responsibilities, and performance objectives. This can make doctors feel annoyed and create the idea that administrative concerns take precedence over clinical care over time.

8.2 Techniques for matching compliance and care

Organisations that effectively match compliance with care tend to emphasise pragmatic integration above policy development, by integrating compliance into routine operations.

When compliance requirements are shown as part of providing responsible care rather than as outside enforcement, they are more easily embraced. This calls for ongoing reinforcement and visible leadership.[20]

Figure 7: Mastering compliance with care

Emphasising pertinent, continuous learning

With evolving regulatory frameworks fixed training rapidly loses relevance. 'One-size-fits-all' training courses have proven to be less effective than short, scenario-based learnings connected to actual operational challlenges.

Utilising audits as development tools

Regular internal evaluations, when framed as learning tools rather than fault-finding ones, can reveal hazards early and promote ongoing improvement.

Leveraging technology with purpose

Digital tools—ranging from compliance tracking systems to electronic health records—can lower administrative load. However, badly designed systems typically tend to create new risks instead of addressing current ones.

16. https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf

17 https://www.digitalhealthnews.com/pm-modi-calls-on-indian-ai-startups-to-prioritize-healthcare-innovations

18. https://www.oecd.org/en/publications/health-data-governance-for-the-digital-age_68b60796-en.html

19. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

20. https://www.oecd.org/en/publications/health-data-governance-for-the-digital-age_68b60796-en.html

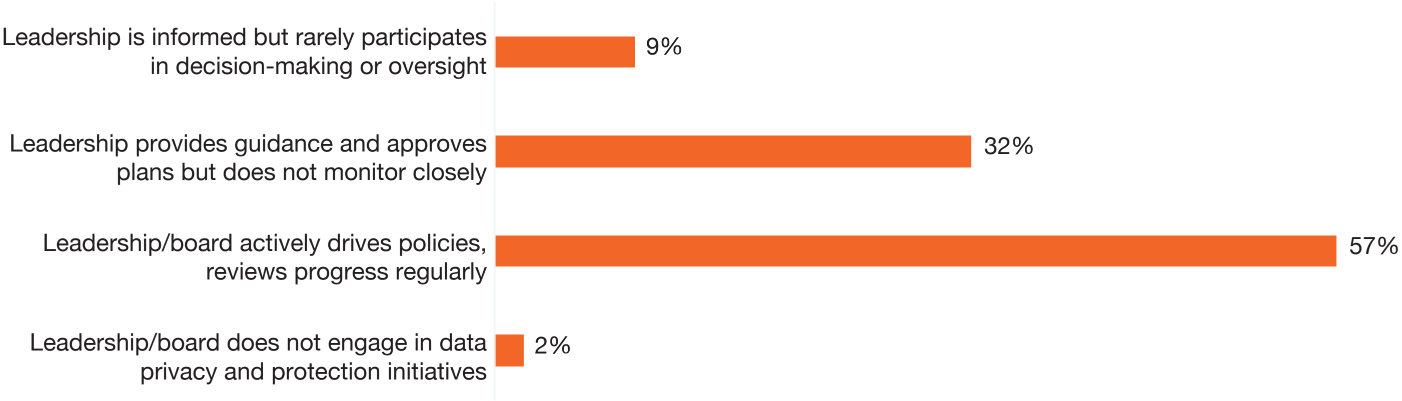
8.3 Leadership's role in balancing care and compliance

The way the company sees compliance and quality is largely determined by leadership conduct. Leaders that attend compliance meetings recognise the importance of these responsibilities. Building trust requires a leader to confront, probe, and reason others' decisions while adhering to the same standards. Patient confidence, moral conduct, and staff involvement in medical settings all rely on their trust.

Rising challenges and future trends point to the fact that a robust compliance culture largely relies on good leadership. According to PwC's Global Compliance Survey, 55% of managers think compliance initiatives work best when senior executives show how important quality and ethics are in a business. Many times, this is known as the 'top tone'. Companies with stronger compliance cultures are also far more likely to factor compliance into major commercial decisions. Open leadership and clear responsibility help build trust, as 59% of the respondents reported greater confidence in compliance-led decision-making owing to better co-ordination.[21] In healthcare, disciplined leadership that establishes systems, processes, and workplace settings where both can thrive is essential for offering great patient care while adhering to legal and ethical standards—choosing one above the other is irrelevant.

Figure 8: Leadership overview

What is the level of leadership or board oversight for patient data privacy and protection initiatives within your organisation?



57% of respondents of a PwC survey state that boards and senior executives track progress along with creating operational standards, whereas 32% receive guidance without any further supervision. The survey results show that only 2% of respondents believe there is no backing from leadership. Moreover, governance practices need improvement because they create operational constraints. The survey also found that 9% of respondents believed leaders possess the knowledge used in their work.

Going forward, organisations should:

- Concentrate on ongoing scenario-based learning that keeps pace with evolving legislative requirements.
- Use audits as developmental research instruments to identify potential dangers and drive organisational growth.
- Use technology with purpose to close their existing gap and reduce paperwork.

Poorly executed systems create new risks for organisations. The combination of these elements enables companies to shift from waiting for problems to developing active governance systems.

[21] https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

09 Way forward

The sections covered highlighted that the transformation of the India's digital health scenario—through various government initiatives including the ABDM and DPDP Act, 2023—has made data privacy, consent, and security the core determinants of growth and innovation in the healthcare ecosystem. With guardrails in place, the governance structure of health data has been redesigned, following a privacy-first approach that is built on uncompromising standards of individual dignity and patient agency.

In this evolving landscape, structured approach to data governance is critical and support from cyber and risk specialists can help stakeholders and organisations understand the compliance expectations and help them integrate the risks more effectively in their operational workflow.

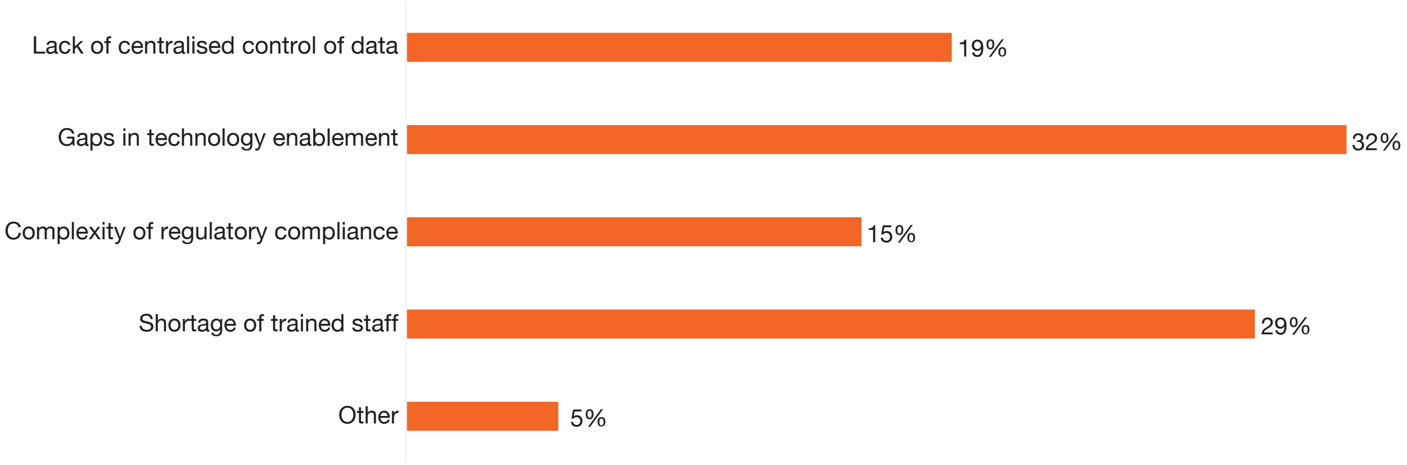
Building on this foundation, industry insights emerging from the PwC survey offer more clarity on the readiness of organisations to operate in this privacy-first environment. Findings from the survey reveal that 32% respondents feel the current gap in the technology enablement is the biggest challenge to managing data privacy, closely followed by 29% who believe shortage of trained staff to be a significant factor—representing an ecosystem with uneven functional capabilities (Figure 10).

The pattern reflects both policy and capability gaps. Scaling of digital care requires upskilling of the workforce, centralised data governance, and privacy-focused technology. Expert-led programmes in consent mangement, data protection, and compliance readiness can fast-track growth by preparing teams with skills and tools for proper management of such large-scale data.

Addressing these barriers will determine and shape the maturity of India’s digital healthcare ecosystem.

Figure 9: Challenges in managing data privacy

What do you consider to be the most significant challenges in managing data privacy across your organisation, particularly in the context of evolving data privacy regulations in India?

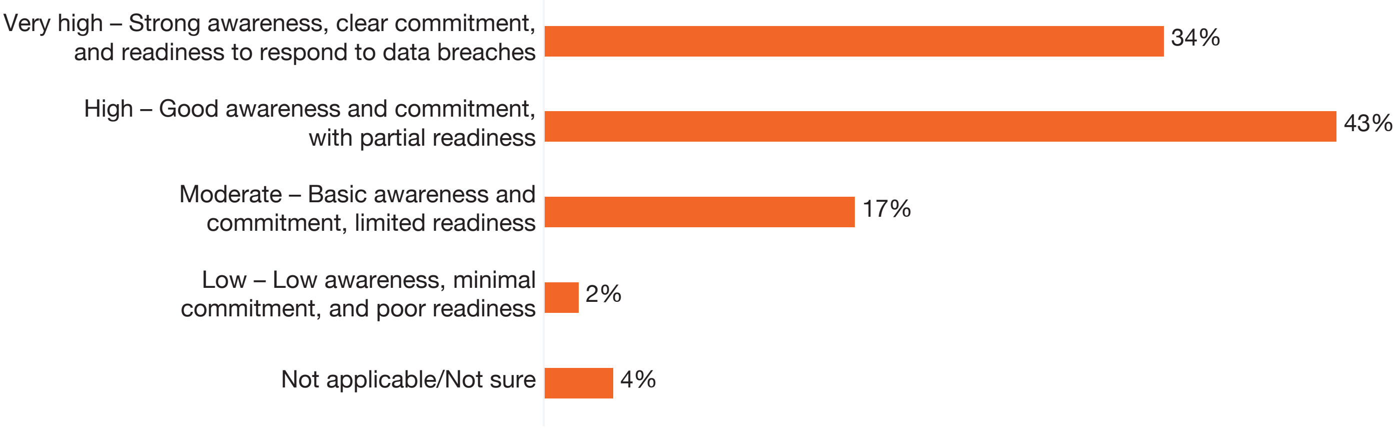


As shown in Figure 11, 43% of respondents have assessed their readiness to handle data breaches as 'High' and 34% as 'Very high', while 17% indicate moderate preparedness. A small portion of the organisations acknowledged 'Low' readiness. These insights demonstrate how strategic actions must increase operational strength for digital health ecosystem to mature.

Independent assessments, incident response readiness, and simulation exercises can help organisations validate their self-reported statuses with actual real-world preparedness.

Figure 10: Organisation readiness to data breaches

How would you assess your organisation's awareness, commitment, and readiness to responsibly handle and respond to potential patient data breaches?



Breach readiness forms the safety net for a digital ecosystem. While the self-reported levels of breach-readiness appear strong on paper, it is essential to operationalise drills, monitoring activities, and third-party assurances to build ecosystem-wide synergy and embed compliance in everyday workflows.

To move towards a resilient, privacy-first, citizen-centric digital healthcare ecosystem, organisations will need to deliberately strengthen the **four interconnected pillars of the ecosystem.**

Firstly, the role of **people** is fundamental. A privacy-first healthcare ecosystem begins with the people—healthcare providers, administrators, frontline workers along with the technology teams—who must evolve into privacy-aware practitioners, keeping data sensitivity and security as a fundamental part of their protocols and workflows. The survey features a shortfall of trained personnel, which reinforces the urgency to educate, train, and embed privacy into day-to-day protocols and workflows. This can be done by expanding staff capabilities and securing data handling and breach responsiveness. Expanding consent literacy among the staff and embedding data privacy practices and responsibility in the culture of the organisation will further play a crucial role in building trust and ensure practices like telemedicine, remote patient monitoring, digital OPDs, or 5G clinics operate without any informational vulnerabilities.

Secondly, **processes** need to be redesigned to strengthen patient agency throughout the care lifecycle. As the survey suggests, organisations need to shift from fragmented capturing of consent to a continuous data-sharing, patient-centred activity across registrations, diagnostics, teleconsultations, insurance and claim sharing. Organisations should integrate data minimisation in their processes, clearly redefine data retention periods, and have a thorough privacy-by-design review for every product and process to move beyond compliance and build system-wide consistency in how data is managed. This procedural discipline is crucial not only for the regulatory compliance view but for reinforcing the ethical core of digital health.

Thirdly, **digital infrastructure and technology** must have a secure-by-default capability, supporting India's expanding digital footprint. The survey findings on technology enablement gaps underline the need for organisations to strengthen their stance by reinforcing end-to-end data encryption, impose stricter identity and access management rules, have consent governing APIs that reflect the DPDP Act's accountability standards, along with adherence to federated data storage guidelines to ensure that digital health data remains safe when digital penetration scales. Furthermore, the future of AI in healthcare must be built on anonymised datasets and learning models that align with DPDP Act's research and statistical processing requirements and exemptions, while preventing identification risks.

Finally, **awareness** must be the combining factor empowering citizens within this digital transformation. The readiness landscape depicted in Figure 10 reveals that there remains substantial scope for improvement in terms of public awareness and clarity. Transparent communication on how personal data will be collected, used, stored, and shared—supported by easy-to-understand consent frameworks, multilingual interfaces, and targeted public campaigns—will clarify digital health for all stakeholders in the digital health ecosystem.

With structured frameworks and citizen-centric privacy design support, organisations can build public trust and make digital healthcare more transparent and accessible.

In conclusion, digital healthcare in India is entering a consolidation phase where interoperability, AI-driven insights, and nationwide health data portability will bring unprecedented value. But its sustainability will depend on how organisations are able to uphold privacy, strengthen cybersecurity practices, and bridge care gaps across the demographic divide in the country.

With inclusive design and cautious execution, India can develop a digital healthcare landscape that is built on technological advancement with a privacy-first approach, thus protecting rights and expanding access to universal dignified care for the future.

About PwC

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Heena Vazirani
Partner – Privacy, Cyber & Digital Risk
PwC India
heena.vazirani@pwc.com

Sayantan Chatterjee
Partner – Digital Strategy
PwC India
sayantan.chatterjee@pwc.com

Authors

Krishna Veni Pandelapalli
Abhishek Tiwari
Ishita Datta
Akshay Ramani
Pratick Chaudhary
Rima Agarwal
Venkatesh Babu
Muskan Joshi

Editorial

Rashi Gupta

Design

Kirtika Saxena

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

KS/February 2026-M&C 51463