



The privacy prescription

Impact of DPDP Act and rules in healthcare and life sciences sector

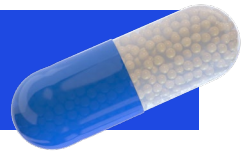


kpmg.com/in

KPMG. Make the Difference.

December 2025

Implications of DPDPA and action plan



The **Digital Personal Data Protection (DPDP) Act, 2023**, along with the 2025 Rules, introduces a stringent privacy regime for India's healthcare and life sciences sector, which handles highly sensitive health data.

Key Implications

- **Consent-centric processing:** Explicit, informed consent is mandatory for collecting and using patient data. Blanket or implied consent is invalid
- **Patient rights:** Individuals can access, correct, and erase their health data, systems must be designed to ensure compliance
- **Data minimisation and purpose limitation:** Only necessary data for treatment or research can be processed; secondary use without consent is prohibited
- **Governance and accountability:** Appointment of Data Protection Officers (DPOs), breach reporting within 72 hours, and Data Protection Impact Assessments (DPIAs) for high-risk activities are mandatory.

Leveraging DPDPA for advantage



Build patient trust

Transparent data practices enhance credibility and strengthen patient-provider relationships



Enable ethical innovation

Compliance enables responsible use of AI, telemedicine, and research while safeguarding privacy



Global alignment

General Data Protection Regulation (GDPR) - like standards position Indian healthcare for international collaborations and clinical trials.



Medical emergencies and public health

Processing without consent is allowed during emergencies, epidemics, or for health services where delay could harm patients



Child health data

Hospitals, clinics, and allied professionals can process children's data without parental consent if necessary for health protection. These exemptions ensure care delivery is not delayed by administrative consent cycles, but security and breach-notification obligations still apply.

Immediate actionables:



01

Audit data practices

Map patient data flows, evaluate consent management mechanisms, assess and identify the security gaps

04

Strengthen cybersecurity

Encrypt health data, enable multi-factor authentication, and prepare for 72-hour breach reporting

05

Plan for SDF obligations

Large hospitals and health-tech firms must appoint Data Protection Officer, conduct audits, and Data Protection Impact Assessment.

02

Consent management

Ensure explicit, informed, and revocable consent across all touchpoints

03

Implement Privacy-by-design

Embed compliance in EHR systems, telemedicine platforms, and mobile apps

06

Future-proof operations

Align with global standards (GDPR, HIPAA) and adopt consent orchestration tools

KPMG in India got you covered...

KPMG in India's Privacy Offerings

**Privacy
management
office**

**Privacy-by-
design
implementation**

**Privacy
platform
automation**

**Designing
consent
management
architecture**

**Data Principal
Rights
enablement**

**Privacy-driven
customer
experience
enhancement**

**Personal data
breach
simulation
programs**

**Data
Processing
Agreement
compliance
reviews**

Acknowledgements

We are extremely grateful to senior leaders from the industry, subject matter experts, and KPMG in India team members for extending their knowledge and insights to develop this document.

Contributors:

Shikha Kamboj

Vipul Ubale

Rupak Nagarajan

Ayushi Dasgupta

Shashwati Alkari

Mala Lahoti

Nivesh Jain

Arshi Ali

Aditya Singh



KPMG in India contacts:

Akhilesh Tuteja
Global Head – Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner, HoF - Digital Trust
E: atulgupta@kpmg.com

Lalit Mistry
Partner & Head – Healthcare
E: lalitmistry@kpmg.com

Nitin Shah
Partner & Head
Cyber Strategy and Governance
E: nitinshah@kpmg.com

Shikha Kamboj
Partner Digital Trust
National Lead, Data Privacy and Ethics
E: skamboj@kpmg.com

Rupak Nagarajan
Partner, Digital Trust
Data Privacy and Ethics
E: rupak@kpmg.com

Vipul Ubale
Associate Partner, Digital Trust
Data Privacy and Ethics
E: vipulubale@kpmg.com

Kanika Jain
Associate Partner, Digital Trust
Data Privacy and Ethics
E: kanikajain@kpmg.com

kpmg.com/in



Access our latest insights
on KPMG Insights Edge

Follow us on:
kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the quoted third parties and do not necessarily represent the views and opinions of KPMG in India.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai – 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

This document is for e-communication only.