jsa
advocates & solicitors

JSA Prism

Privacy and Data Protection

Digital Personal Data Protection Act

Edition XII

January 2025

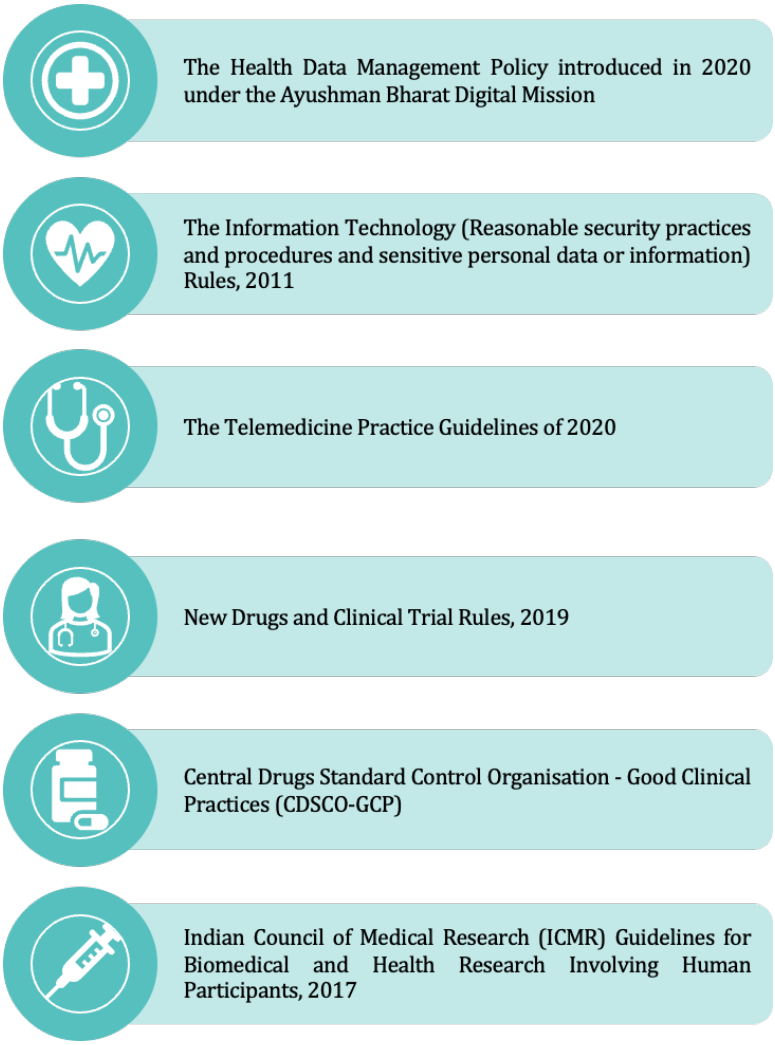
Navigating privacy requirements for healthcare and pharmaceutical sectors

The healthcare and pharmaceutical sectors in India are at a critical juncture concerning data protection and privacy. Despite the growing reliance on digital health records and technology, the regulatory framework remains fragmented to address the complexities of modern healthcare data ecosystems. The Digital Personal Data Protection Act, 2023 ("**DPDPA**") introduces a new paradigm for data protection, but its integration with the healthcare and pharmaceutical sector's unique requirements presents challenges and opportunities. This edition of the Prism series evaluates the DPDPA's impact on healthcare and pharmaceutical sectors, its interplay with existing sectoral guidelines, and the path forward for comprehensive health data governance in India.

The current regulatory landscape governing health data in India

India currently lacks a comprehensive law addressing healthcare or patient data, unlike the United States' Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). Enacted to safeguard patient privacy, regulate the use and disclosure of protected health information, and promote efficiency and interoperability in healthcare, HIPAA serves as a robust framework for managing health information in the USA. In India, an attempt to introduce similar protections through the Digital Information Security in Healthcare Act, 2018 focused on regulating digital health data with strict security, consent, and accountability measures has failed to progress. Instead, the healthcare sector remains governed by a patchwork of sectoral regulations. Instead, there is a patchwork of regulations that apply to processing health and patient data.

Overview of key sectoral regulations applicable to this sector currently



1. **The Health Data Management Policy ("HDM Policy")**: The HDM Policy v.2, released in 2022, by the Ministry of Health and Family Welfare, sets the minimum standards for privacy and data protection within the Ayushman Bharat Digital Mission ecosystem. The HDM Policy mandates that no health data be shared with entities, including insurance and pharmaceutical companies, without the individual's consent. It imposes purpose-based limitations on data sharing and requires health information users to refrain from further disclosing data without the data principal's consent. Additionally, shared data must not be stored beyond the period necessary for the specified purpose, and the principle of data minimisation must be adhered to by entities receiving the data.
2. **The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules")**: The SPDI Rules, issued under Section 43A of the Information Technology Act, 2000, establish a framework for handling sensitive personal data, including health information. The SPDI Rules define Sensitive Personal Data or Information ("**SPDI**") to include medical records, biometric information, and physical or mental health conditions. Organisations collecting SPDI are required to publish a privacy policy, clearly disclose their data collection and processing practices, and secure informed consent from individuals before collecting or sharing their data. The rules emphasise implementing stringent security measures, such as encryption and access controls, and require organisations to appoint a grievance officer to address complaints. Non-compliance can attract civil liability for negligence, underscoring the SPDI Rules' role in ensuring accountability and data protection, particularly in sectors like healthcare that handle highly sensitive information. When the DPDPA comes into force, the SPDI Rules will automatically be repealed.
3. **The Telemedicine Practice Guidelines of 2020**: The Telemedicine Guidelines emphasise that Registered Medical Practitioners ("**RMPs**") must adhere to the Indian Medical Council Act ("**IMC Act**") and professional ethics

regarding patient privacy and confidentiality. RMPs must also comply with relevant data protection laws, including the Information Technology Act, 2000 and take reasonable care when selecting services to prevent breaches of patient confidentiality. RMPs will not be held responsible for confidentiality breaches due to technology or third-party failures if proper care is exercised. Misconduct, including forcing teleconsultations when in-person is requested, misusing patient data, and violating privacy laws, is strictly prohibited. Penalties for violations are in line with the IMC Act and other applicable laws.

4. **The New Drugs and Clinical Trial Rules, 2019 ("CTR")**: CTR forms the core regulatory framework for conducting clinical trials in India. These rules govern the approval process, ethical considerations, and conduct of clinical trials. Key provisions include the need for ethics committee approval before initiating a trial and the submission of trial protocols to the Central Drugs Standard Control Organisation ("**CDSCO**") for review. CTR also mandate compliance with international standards to ensure the integrity of data and the safety of trial participants. A critical requirement under the CTR is the obligation to obtain informed consent from participants, ensuring they are fully informed about the risks, benefits, and purpose of the trial before their participation.
5. **CDSCO – Good Clinical Practices Guidelines ("CDSCO - GCP Guidelines")**: The CDSCO – GCP Guidelines outline the ethical and scientific quality standards for clinical trials. These CDSCO – GCP Guidelines are in line with international best practices and focus on protecting the rights and safety of participants while ensuring the reliability of trial data. The CDSCO – GCP guidelines emphasise the need for strict adherence to safety protocols, confidentiality, and transparency in reporting trial results. They also reinforce the requirement for informed consent to ensure participants understand the potential risks and benefits associated with their involvement in clinical trials.
6. **Indian Council of Medical Research Guidelines for Biomedical and Health Research Involving Human Participants, 2017("ICMR Guidelines")**: ICMR Guidelines provides additional ethical guidance for biomedical research in India. The ICMR Guidelines focus on the protection of human participants and emphasise the need for informed consent before any research is conducted. They ensure that participants are not coerced or misled and that their rights are upheld throughout the research process. The ICMR Guidelines also establish standards for research ethics committees, data management, and the dissemination of results, all while ensuring compliance with national and international ethical standards in health research.

With the DPDPA now in place, healthcare and pharmaceutical entities must navigate these fragmented regulations and the broader obligations under the DPDPA.

Transformative implications of the DPDPA on the healthcare and pharmaceutical sectors

The DPDPA introduces comprehensive provisions to strengthen data protection across sectors, including healthcare. The DPDPA mandates a higher degree of accountability for Significant Data Fiduciaries ("**SDFs**") which may include entities processing large volumes of sensitive data such as health data. Health data, while not explicitly classified as sensitive personal data under the DPDPA, may be treated with the same level of protection due to the context provided by the SPDI Rules. This ensures stricter regulations on its processing, storage, and sharing.

The following points outline the key provisions of the DPDPA that influence the regulation of health and patient data in India.

1. **Consent**

   A central feature of the DPDPA is its requirement of specific, informed, affirmative consent, which places the patient at the core of its protections. The DPDPA requires explicit, informed consent from individuals for the collection and processing of their health data. This empowers patients to make well-informed decisions about how their data is used and shared. The DPDPA also provides individuals with the right to withdraw their consent at any time, further reinforcing their control over personal information. For healthcare entities, this means establishing patient-centric mechanisms for obtaining and managing consent, which ensure that data collection aligns with lawful, specific purposes.

2. **Processing for legitimate uses**

   The DPDPA provides for the processing of personal data without explicit consent in certain situations.

   In the context of healthcare, the DPDPA permits data processing during medical emergencies involving threats to life or health. It also allows processing to provide medical treatment or health services during public health crises, such as epidemics or disease outbreaks. These provisions enable delivering lifesaving care without the requirement of going through a consent mechanism.

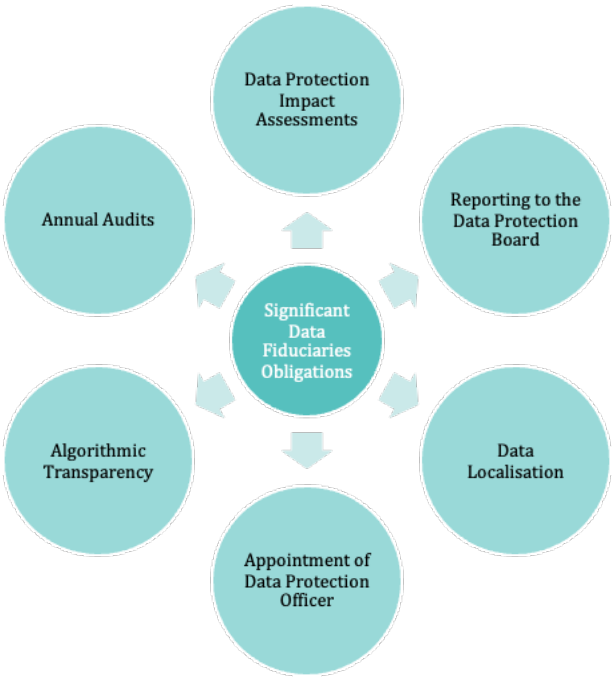
3. **Security obligations for data fiduciaries**

   The DPDPA requires data fiduciaries to implement measures to protect personal data from breach. The draft DPDP Rules 2025 ("Draft Rules") enumerate some security measures including encryption, obfuscation, or virtual tokens to secure personal data, access control mechanisms maintaining logs and monitoring access patterns and reviewing them to detect unauthorised access. In the event of a breach or compromise, data fiduciaries must have measures in place to continue processing data, such as data backups, and ensure that the breach does not hinder the ongoing availability or integrity of the data.

   The DPDPA and Draft Rules also make it the data fiduciary's responsibility to ensure that data processors also implement appropriate technical and organisational measures for data protection and comply with the same high standards of data protection.

4. **Enhanced obligations for SDFs**

   A key feature of the DPDPA is the introduction of a class of SDFs, which is likely to include entities handling such sensitive data like health or patient data. These SDFs have enhanced obligations under the DPDPA and must implement stringent safeguards to protect patient privacy.



SDFs are required to conduct annual data protection impact assessments to identify and mitigate risks associated with their processing operations, particularly in scenarios involving high-risk data usage. Annual audits are also mandatory, with significant findings required to be reported to the Data Protection Board of India ("**Board**"), thereby enhancing regulatory oversight. To promote fairness, SDFs are obligated to ensure algorithmic transparency, which includes measures to detect and prevent biases in automated decision-making processes. Data localisation measures may also apply, requiring critical or SPDI to be stored within India to strengthen data security and uphold sovereignty. Furthermore, SDFs must establish efficient grievance redressal mechanisms to address data principals' complaints in a timely manner and appoint a Data Protection Officer in India to oversee compliance and act as a liaison with the Board. These obligations reflect the DPDPA's focus on safeguarding personal data, promoting transparency, and ensuring accountability.

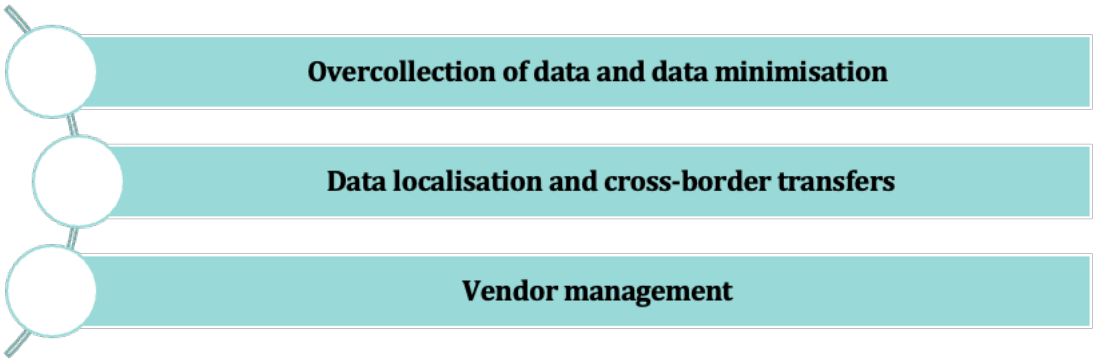
5. **Processing data of children and persons with disability**

As a rule, the DPDPA requires data fiduciaries to obtain verifiable consent from a child's parent or lawful guardian before processing the child's personal data. This consent must be acquired with due diligence to verify the identity of the parent or guardian, using reliable identity and age details or government issued ID. For the healthcare and pharma sectors, this means that any collection or processing of children's personal health data will require parental consent protocols that can be verified. Additionally, the DPDPA also prevents tracking and behavioural monitoring of children.

In view of any imminent threats to the health of a child, the Draft Rules do provide for exceptions to the rule of consent and bar on tracking and behavioural monitoring. A data fiduciary who is a clinical establishment, mental health establishment, healthcare professional or an allied healthcare professional like a trained individual supporting diagnosis, treatment, and healthcare plans, does not need parental consent and may undertake behavioural monitoring of children or targeted advertising directed at children to the extent necessary for the protection of her health. What will be considered 'necessary' and 'for the protection of health' will need to be justified by the data fiduciaries. It will thus become important to have internal protocols identifying situations where the rule on consent and behavioural monitoring/tracking can be ignored by the healthcare establishment or health professionals.

Addressing operational challenges in privacy in healthcare

The healthcare sector may face some unique challenges in aligning with the DPDPA's compliance requirements.



1. **Overcollection of data and data minimisation**

One of the key concerns in the healthcare sector is the over-collection of data, particularly during patient onboarding or diagnostic processes. Historically, healthcare providers may have collected large volumes of data to ensure comprehensive coverage of potential medical needs. However, under the DPDPA, healthcare providers must reassess their data collection practices to ensure that only the data necessary for the intended medical purpose is collected and processed. Healthcare providers and allied providers will need to establish clear criteria

for data collection, map it to certain diagnostic or treatment plans, limit unnecessary data requests, and ensure that any additional data collected is strictly essential for patient care. This shift will require continuous training, updates to internal processes, and close monitoring to ensure that data minimisation is adhered to at every stage of patient interaction.

2. **Data localisation and cross-border transfers**

   Additionally, healthcare providers may have to navigate the operational complexities of cross-border data transfers. Many providers depend on global systems for storing, analysing, and sharing patient data, leveraging international expertise to enhance healthcare delivery. For SDFs, the Central Government can restrict the transfer of personal data to countries or territories outside India and in some cases even mandate data localisation. It will thus become important for all providers in the healthcare ecosystem to understand where data is flowing and have mechanisms to flow down transfer restrictions, if needed. Localisation mandates also necessitate substantial investment in local infrastructure, reassessment of global partnerships, and the establishment of India-based storage and processing systems. By aligning operations with these localisation requirements, healthcare providers can balance regulatory compliance with operational efficiency in a rapidly evolving data governance landscape.

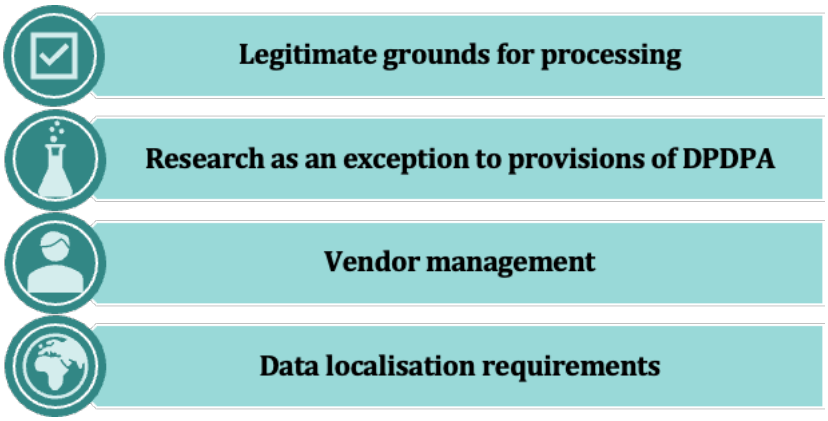
3. **Vendor Management**

   In addition to the challenges of data protection compliance and cross-border data transfers, vendor management is another crucial operational consideration for healthcare providers. Healthcare organisations often collaborate with partners and third-party vendors for a variety of services, such as data storage, software solutions, insurance and analytics. These third parties may have access to sensitive patient data, raising the need for stringent data protection measures in contracts with them.

   The DPDPA requires that when a healthcare provider, as a data fiduciary, engages a data processor, they remain responsible for the processor's acts and omissions. Vendors are only allowed to process personal data under the instructions of the data fiduciary in an appropriate contract. The data fiduciary also has the responsibility to ensure that their processors are keeping data safe and following the instructions of the fiduciary for erasure. The Draft Rules also emphasise the need for proper contracts and compliance checks to ensure third-party vendors meet the required data security standards. This makes it crucial for healthcare providers to implement robust vendor management practices from due diligence to efficient contracts to audits.

Challenges and opportunities in privacy in the pharmaceutical sector

DPDPA presents some challenges for the pharmaceutical sector too, particularly in handling sensitive patient data and data relating to clinical trials. Pharmaceutical companies process large volumes of patient data, including health records and clinical trial data. With the DPDPA, companies must adapt their existing processes and technologies to ensure compliance, especially in patient consent management.



1. **Legitimate grounds for processing**

   Under the DPDPA, several legitimate grounds for processing personal data without consent are explicitly applicable to delivering healthcare, such as responding to medical emergencies, providing treatment during epidemics or disease outbreaks, and ensuring safety during disasters. These provisions allow healthcare providers to process data directly related to patient care and public health without explicit consent. However, the pharmaceutical sector operates differently, often focusing on clinical trials, drug development, and long-term data collection rather than immediate healthcare delivery. These activities typically do not fall under the same exemptions. For instance, while a pharmaceutical company may process data during a government-mandated vaccination program under the public health exception, ongoing clinical trials or pharmacovigilance activities may still require explicit consent from individuals. The distinction lies in the scope of application i.e., healthcare providers directly deliver care, whereas pharmaceutical companies are often a step removed. This creates a complex compliance landscape for pharma companies, requiring them to carefully evaluate which legal grounds apply to their operations and implement robust consent management systems to address activities that fall outside the scope of healthcare exemptions. Failure to do so risks non-compliance with the DPDPA's stringent requirements.

2. **Research as an exception to provisions of DPDPA**

   Under the DPDPA, personal data being processed for research, archiving, or statistical purposes, is exempted from the provisions of the DPDPA, provided the processing is carried out in accordance with some standards that the Draft Rules prescribe.

   In the pharmaceutical sector, this exemption is crucial for activities such as clinical trials and medical research, where data usage often extends beyond the scope of initial collection. Pharmaceutical companies can process sensitive health data for research purposes, but they must ensure compliance with the standards the Draft Rules lay down, including ensuring data accuracy, notifying data principals of their rights, safeguarding the data through robust security measures, implementing grievance redressal and ensuring that the processing remains proportionate and necessary for the research objectives.

3. **Vendor management**

   Vendor management is a key operational concern for pharmaceutical companies too. Pharma organisations regularly collaborate with external vendors, distributor or partners for marketing or manufacturing services.

   The DPDPA requires that when a healthcare provider, as a data fiduciary, engages a data processor, they remain responsible for the processor's acts and omissions. Vendors are only allowed to process personal data under the instructions of the data fiduciary in an appropriate contract. The data fiduciary also has the responsibility to ensure that their processors are keeping data safe and following the instructions of the fiduciary for erasure. The Draft Rules also emphasise the need for proper contracts and compliance checks to ensure third-party vendors meet the required data security standards. This makes it crucial for healthcare providers to implement robust vendor management practices from due diligence to efficient contracts to audits.

4. **Data localisation requirements**

   The DPDPA specifies that the Central Government may proscribe personal data transfer to certain countries or regions. The Draft Rules go a step further and lay down that the Central Government may also prescribe certain requirements for transfer of data. Additionally, for SDFs that Central Government may also mandate that all data, including the traffic data be localised only in India.

   Localisation mandates necessitate substantial investment in local infrastructure, reassessment of global partnerships, and the establishment of India-based storage and processing systems.

   It thus becomes critical for pharma companies to understand and map their data flow, not only across their systems but also those of their partners and vendors.

Privacy issues in deploying Artificial Intelligence in the healthcare and pharmaceutical sectors

In the healthcare and pharmaceutical sectors, Artificial Intelligence ("**AI**") holds great promise for enhancing patient care, improving operational efficiencies, and advancing medical research. AI is being utilised in drug discovery, diagnostics, clinical decision-making, supply chain management, and clinical trials, among other areas. By analysing large datasets, AI accelerates research, aids in the identification of potential drug candidates, and optimises clinical trial designs, ensuring safer and more effective treatments.

However, as AI's role in processing personal health data expands, it raises significant data privacy concerns. A primary issue is the sheer volume of personal health data being processed by AI systems. This not only increases the risk of data breaches but also raises compliance challenges. The DPDPA emphasises data minimisation, a principle that requires that personal data collected be limited to what is necessary for the intended purpose. The growing use of AI in healthcare intensifies the need to ensure that only relevant data is processed and retained, in compliance with this core principle.

AI algorithms, especially those deployed for processing personal health data, must also be scrutinised to ensure they do not pose a risk to data principals' rights. The Draft Rules require SDFs to carry out due diligence and verify that the algorithmic software used for processing personal data—whether for storage, transmission, or sharing—does not create unintended risks, such as discriminatory outcomes or breaches of privacy.

These rules necessitate that companies employ strict oversight to mitigate any harm to individuals and ensure compliance with the DPDPA's provisions on data protection and privacy. This may require carrying out an impact assessment before AI is deployed for any use.

Consumer health-tech

The use of consumer health technologies, such as wearables and mobile health apps, presents different privacy challenges, particularly in terms of data overcollection and the frequent transfer of data across various platforms. These technologies often collect continuous, real-time health information, which, if not properly safeguarded, can be vulnerable to unauthorised access, misuse, or breaches. Furthermore, as the data is typically processed or shared with multiple third-party vendors and platforms, the risk of data leakage, especially in cross-border scenarios, becomes more pronounced.

Under the DPDPA, data fiduciaries hold primary responsibility for ensuring compliance with the DPDPA, even in instances where data processing is carried out by third-party processors. According to the provisions of the DPDPA, a data fiduciary must ensure that any processing undertaken by its processors on its behalf complies with the law. The fiduciary remains accountable for the actions of these processors, irrespective of any agreements made or the failure of the data principal to uphold their duties under the DPDPA. This legal responsibility necessitates thorough oversight and due diligence by data fiduciaries, requiring them to ensure that processors adhere to data protection principles such as data minimisation, purpose limitation, and safeguarding sensitive health data from unauthorised access or misuse.

The path forward for health and pharma data governance

The DPDPA provides a comprehensive framework for data protection and its true effectiveness will depend on its harmonious integration with existing sectoral regulations. While sectoral regulations currently address important aspects of health and patient data management, they lack the detailed requirements outlined in the DPDPA.

Organisations will need to invest time, resources, and expertise to adapt their processes and meet the stringent data protection standards set by the DPDPA. Additionally, the Draft Rules introduce further refinements to these requirements, requiring continuous assessment and adjustment by healthcare and pharmaceutical entities to ensure full compliance.

Infotech Practice (Privacy and Data Protection)

Our team understands the importance of data privacy in today's digitally interconnected world. We have dedicated our practice to ensuring that your and your customers' personal and business data remains secure, compliant, and respects the sovereignty of individuals and jurisdictions globally.

We prioritise creating bespoke solutions tailored to your business needs. We recognise that every business has unique data privacy challenges, and we use our deep understanding of international and domestic regulations to provide you with the most effective and robust legal strategies. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. Our Technology Law Practice group has successfully worked with several multinational organisations for the structuring and roll-out of privacy and information-security programs. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements.

This Prism has been prepared by:

Akshaya Suresh
Partner

Drishya A. Kamath
Associate

Chambers TOP RANKED Asia-Pacific 2025 JSA	Chambers TOP RANKED Global 2024	IFLR1000 TOP TIER FIRM 2024
18 Practices and 41 Ranked Lawyers	7 Ranked Practices, 16 Ranked Lawyers --- Elite – Band 1 - Corporate/ M&A Practice --- 3 Band 1 Practices --- 4 Band 1 Lawyers,1 Eminent Practitioner	12 Practices and 50 Ranked Lawyers
The Legal 500 UNITED KINGDOM TOP TIER 2024 14 Practices and 38 Ranked Lawyers		
asialaw OUTSTANDING FIRM 2024 20 Practices and 22 Ranked Lawyers	The Legal 500 Ranked Among Top 5 Law Firms in India for ESG Practice	GCR 100 2025 The guide to the world's leading competition practices Recognised in World's 100 best competition practices of 2025
INDIA BUSINESS LAW JOURNAL BEST OVERALL LAW FIRMS 2024 Among Top 7 Best Overall Law Firms in India and 11 Ranked Practices --- 11 winning Deals in IBLJ Deals of the Year --- 11 A List Lawyers in IBLJ A-List - 2024	ALB Asia M&A Ranking 2024 – Tier 1 --- Employer of Choice 2024 --- Energy and Resources Law Firm of the Year 2024 --- Litigation Law Firm of the Year 2024 --- Innovative Technologies Law Firm of the Year 2023 --- Banking & Financial Services Law Firm of the Year 2022	vahura **Ranked #1** **The Vahura Best Law Firms to Work Report, 2022** --- Top 10 Best Law Firms for Women in 2022 BENCHMARK LITIGATION 7 Practices and 3 Ranked Lawyers

For more details, please contact km@jsalaw.com

Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi