

Regulatory Divergence in Digital Healthcare: Corporate Governance, Risk Mitigation, and Data Privacy Liabilities for Transnational Telehealth Providers Under the EU GDPR and India's DPDPA

An Empirical and Comparative Legal Study

Faisal Yaseen¹, Fouzan Shah²

¹Assistant Manager, Medanta

²Advocate, Delhi High Court

Author Disclosure: Although the first author is affiliated with Medanta, no data, information, materials, or resources from Medanta were used in the preparation of this manuscript. The analysis, findings, and views expressed are based solely on publicly available regulatory texts, published enforcement and market data, and the primary survey described in Section 3.3.

Abstract

Telehealth companies that operate across borders handle sensitive patient data clinical records, biometric information, and behaviour patterns for patients in both the European Union and India. These two regions have very different data protection laws, in terms of how the rules are designed, how they are enforced, and who can be held responsible when something goes wrong. This paper compares the corporate governance duties, risk-management practices, and data privacy liabilities faced by telehealth companies that must follow both the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDPA), which is now being put into effect through the Digital Personal Data Protection Rules, 2025. The study uses GDPR enforcement records, market data on India's telehealth sector, and a survey of 42 compliance officers at telehealth companies. From this, it builds a simple index comparing how strict each law is, and measures how much compliance risk officers feel across six areas of their work. The findings show that GDPR carries a much higher risk of direct fines and has more experienced regulators enforcing it. DPDPA's biggest risk, by contrast, comes from unclear rules particularly around moving data across borders, reporting data breaches on time, and deciding which companies count as "Significant Data Fiduciaries" (a special category under Indian law). The paper argues that companies whose governance structures are built only around GDPR may still have compliance gaps under DPDPA, which focuses heavily on consent and holds company boards directly accountable. It ends by proposing a three-tier governance framework to help companies meet both sets of rules at once.

Keywords: telehealth governance; GDPR compliance; Digital Personal Data Protection Act; cross-border data transfer; healthcare data privacy; regulatory divergence

1. Introduction

Telehealth healthcare delivered remotely, often online started as a temporary fix during the COVID-19 pandemic. It has since become a permanent part of how healthcare is delivered, both in the European Union and in India. India's telehealth market alone is expected to grow from about USD 6.28 billion in 2024 to USD 27.2 billion by 2030 a yearly growth rate of 27.7 percent (Grand View Research, 2025). Meanwhile, the EU's own digital health services keep expanding under its European Health Data Space initiative. But the law has not kept pace with this growth: the rules for moving health data across borders have not been brought into line with each other. This paper calls this problem “regulatory divergence”: a situation where companies operating in more than one country must follow different and sometimes conflicting legal rules for what is really the same activity, namely processing patient data.

The EU's General Data Protection Regulation, or GDPR (Regulation (EU) 2016/679), has been in force since 25 May 2018. It is widely seen as the world's most developed data protection law, and it applies even to companies based outside the EU if they handle EU residents' data. Under GDPR, health data is treated as a “special category” of data requiring extra protection (Article 9), and companies that break the rules can be fined up to EUR 20 million or 4 percent of their worldwide annual revenue, whichever amount is higher (European Parliament and Council, 2016). India's data protection law is much newer, and its constitutional roots trace back to the Supreme Court's recognition of privacy as a fundamental right (Supreme Court of India, 2017). The Digital Personal Data Protection Act, 2023 (DPDPA) received the President's approval on 11 August 2023 (Government of India, 2023), but it had no real legal teeth until the government issued the Digital Personal Data Protection Rules, 2025 on 13 November 2025. These Rules set out a three-phase rollout that will be fully complete by 13 May 2027 (Ministry of Electronics and Information Technology, 2025; IAPP, 2025).

This gap in timing matters. Telehealth companies based in, or serving patients in, both regions have spent almost a decade building their governance systems around GDPR's rules on consent, accountability, and breach reporting. They must now also follow an Indian law that looks similar on the surface but works differently underneath. DPDPA uses a “blacklist” approach to cross-border data transfers meaning transfers are allowed unless a country is specifically named as restricted while GDPR uses the opposite “whitelist” approach, where transfers are blocked unless a country is pre-approved. DPDPA is also enforced by a newly created Data Protection Board of India, not by the twenty-seven experienced national regulators that enforce GDPR across the EU (DPDPA FAQ, 2026).

This paper asks three connected questions. First, how do the corporate governance duties that GDPR and DPDPA place on telehealth providers differ in what they cover, who is held accountable, and how exposed company boards are to liability? Second, what steps are telehealth companies currently taking to manage this gap, and which specific compliance risks do their compliance officers see as most serious? Third, what financial and reputational costs can result from breaking each law, and what do real enforcement cases tell us about how strict each law actually is in practice as opposed to how strict it looks on paper?

The rest of the paper is organised as follows. Section 2 reviews existing research on comparing data protection laws and healthcare compliance. Section 3 explains the research methods used, combining an analysis of enforcement data with a new survey. Section 4 compares the governance and liability rules under each law in detail. Section 5 presents the findings, including the stringency index and survey results.

Section 6 discusses what these findings mean for how companies should govern themselves, and Section 7 concludes with a tiered compliance framework and recommendations.

2. Literature Review

2.1 Comparative Data Protection Scholarship

Researchers who compare data protection laws around the world usually treat GDPR as the global benchmark that other countries' laws are measured against. This influence is sometimes called the “Brussels effect” the idea that because EU rules are so strict and reach so far beyond EU borders, other countries end up following similar standards even without being legally required to. Some commentators see India's DPDPA as a partial example of this effect, since it also applies to any company handling the data of people in India, no matter where that company is based (Privacy World, 2025). At the same time, DPDPA differs from GDPR in important ways for example, it uses “consent managers” as intermediaries, and instead of pre-approving safe countries for data transfer (as GDPR does), it works by naming specific countries as restricted (IAPP, 2025).

Most existing research treats data protection laws as fixed texts on paper, rather than looking at how they are actually enforced in practice. This paper takes the second approach. Data compiled by CMS Law (2026) shows that GDPR fines in the healthcare sector while usually smaller than the large fines that make headlines in the tech sector grew 26 percent in number between the 2025 and 2026 reporting periods. Most of these fines were not for illegal data processing itself, but for having weak technical and organisational security measures. This matters for telehealth governance: it shows that the real risk lies less in how companies get consent from patients (which gets most of the academic and compliance attention) and more in how well they secure their systems data storage, access controls, and oversight of vendors.

2.2 Healthcare Data Governance and the Particular Sensitivity of Telehealth Data

Both laws treat health data as needing extra protection, but they do this differently. Under GDPR, health data is a “special category” (Article 9) that can only be processed if a specific exception applies most often because the patient gave explicit consent, or because the processing is necessary for health or social care provided by someone bound by confidentiality rules (European Parliament and Council, 2016). DPDPA does not create a separate special category for health data at all. Instead, it applies the same general consent-and-notice rules to all personal data. Several practitioners have pointed out that this creates uncertainty about whether health data needs any extra protection beyond ordinary consent under Indian law (DPDPA FAQ, 2026; DPDPA Certificate Course, 2026). This is not just a technical, academic difference it affects how telehealth apps should design their consent screens. If an app uses one single consent process built only to DPDPA's general standard, it may not meet GDPR's higher bar of “explicit consent” for special category data like health records.

Research on healthcare data breaches shows just how high the stakes are. IBM's Cost of a Data Breach Report as summarised by industry analysts found that healthcare has been the most expensive sector for data breaches for fourteen years running. In the United States, the average breach cost USD 7.42 million in 2025, and it took an average of 279 days to detect and contain a breach longer than any other sector (Sprinto, 2025; DeepStrike, 2025). These figures mostly come from the US, where a different law (HIPAA) applies rather than GDPR or DPDPA. Still, they set a useful benchmark. European healthcare GDPR fines look small by comparison averaging EUR 228,161 per fine in 2025 but that does not mean the real risk is smaller. It means that regulatory fines are only one small part of the total cost of a breach.

The rest comes from responding to the incident, legal costs, reputational damage, and disruption to patient care (CMS Law, 2026).

2.3 Corporate Governance Models for Cross-Border Compliance

A smaller, growing body of research looks at how companies should govern themselves when they face more than one data protection law at once. This research generally agrees that effective compliance across two regimes requires a board-level data governance committee, with authority over both laws' officer requirements GDPR's Data Protection Officer (Articles 37–39) and, where it applies, DPDPA's equivalent role for “Significant Data Fiduciaries” under Section 10 (DPDPA FAQ, 2026). This paper builds on that research by surveying real compliance officers to find out which specific governance issues they still see as risky, even after their company has tried to align its policies with both laws a question that has not been tested with real data before.

2.4 Research Gap

This study fills three gaps in the existing research. First, no published work combines real GDPR healthcare enforcement data with DPDPA's enforcement system, which only became operational in November 2025. Second, most comparative research is purely doctrinal it studies the law on paper but does not collect data from real practitioners about how risky they find it. Third, no dedicated study has looked specifically at telehealth, as opposed to healthcare data more broadly, even though telehealth has its own unique risks: data flowing across borders in real time, heavy reliance on third-party platforms, and a mix of clinical and consumer-technology data. This paper addresses all three gaps.

3. Research Methodology

This study uses a mixed-methods design with three parts: a doctrinal comparison of the two laws, an analysis of existing GDPR healthcare enforcement data, and a new survey of compliance and privacy officers at telehealth companies operating across borders. This combination was chosen because the research questions need two different kinds of answers: interpreting what the law says, which is best done through legal analysis, and understanding how practitioners perceive risk, which requires collecting new data especially since DPDPA does not yet have a mature enforcement record to study.

3.1 Doctrinal-Comparative Component

The legal comparison covers seven areas: how far each law reaches beyond its own borders, how consent works, breach-reporting duties, rules on cross-border data transfer, maximum fines, how mature each regulator is, and how broad the rights of patients and users are under each law. Each area is scored from 1 to 5, based on the text of the law itself and supported by official guidance, to build the stringency index shown in Section 5.1. This method turning legal features into numerical scores for comparison is a standard technique in comparative regulatory research. It does involve some judgment calls, which is acknowledged here.

3.2 Secondary Quantitative Component

GDPR healthcare fine data from 2019 to 2025 came from the CMS GDPR Enforcement Tracker Report, Life Science and Healthcare edition (CMS Law, 2026), which collects decisions from data protection authorities across all 27 EU and EEA countries. Market-size figures for India's telehealth and digital health

sectors came from Grand View Research (2025, 2026), the IMARC Group (2026), and Mordor Intelligence (2026). Healthcare breach cost figures came from IBM's Cost of a Data Breach Report, as summarised by Sprinto (2025) and DeepStrike (2025). Because DPDPA's real enforcement record does not exist yet its main provisions do not take full effect until 13 May 2027 the India figure shown in Figure 4 is only an illustrative estimate, based on patterns from India's older Information Technology Act enforcement. It is clearly marked as an estimate and should not be read as an actual DPDPA statistic.

3.3 Primary Survey Component

An online survey was sent to compliance officers, data protection officers, and legal counsel at telehealth companies operating in both the EU and India, between March and June 2026. Respondents were found through professional privacy networks, with participants also referring colleagues (a method known as “snowball sampling”). After removing incomplete responses, 42 valid responses remained ($n = 42$). This is a modest sample, and participants were not randomly selected, so the survey findings should be seen as exploratory rather than representative of every telehealth compliance officer. This fits the fact that DPDPA enforcement was still very new at the time of the survey. Respondents rated six pre-defined compliance risks on a five-point scale (1 = low risk, 5 = severe risk). These six risk areas were chosen after reviewing regulatory guidance and expert commentary. Table 1 summarises who took part.

Table 1: Survey sample characteristics ($n = 42$).

Characteristic	Category	n	% of sample
Organisation headquarters	European Union	16	38.1%
	India	14	33.3%
	Other (US, UK, Singapore)	12	28.6%
Respondent role	Data Protection Officer / DPO equivalent	19	45.2%
	General Counsel / Legal Director	11	26.2%
	Chief Compliance Officer	8	19.0%
	Other senior privacy role	4	9.5%
Organisation size	Under 250 employees	9	21.4%
	250–1,000 employees	17	40.5%

Characteristic	Category	n	% of sample
	Over 1,000 employees	16	38.1%

The limits of this survey method including the sample size, the fact that participants chose to take part rather than being randomly selected, and the timing of data collection before DPDPA enforcement began are discussed in Section 6.4.

4. Comparative Legal Analysis: Corporate Governance and Liability Architecture

4.1 Jurisdictional Scope and Extraterritorial Application

Both laws apply beyond their own borders to telehealth companies, though they use different legal mechanisms to do this. GDPR's Article 3(2) applies to any company processing the personal data of people in the EU, even if that company is based outside the EU, as long as it is offering goods or services to those people (paid or free) or monitoring their behaviour (European Parliament and Council, 2016). DPDPA's Section 3(b) works in a similar way: it applies to processing of digital personal data outside India, as long as that processing relates to offering goods or services to people in India (Privacy World, 2025). So imagine a telehealth company offering video consultations to patients in France and in Maharashtra, using cloud servers based in, say, Singapore. Both laws apply to that company at the same time and independently neither law's reach depends on, or is cancelled out by, the other.

4.2 Lawful Basis, Consent, and the Special Status of Health Data

Under GDPR, a company must have a valid legal reason to process any personal data (Article 6), and for health data specifically, it needs an additional, stronger justification under Article 9(2). In practice, telehealth companies usually rely on either the patient's explicit consent, or the fact that the processing is necessary to provide healthcare by a professional bound by confidentiality (European Parliament and Council, 2016). DPDPA works differently: it applies one single consent standard to all types of personal data (Section 6). That consent must be free, specific, informed, unconditional, clear, and given through a clear affirmative action not assumed from silence (DPDPA FAQ, 2026). The 2025 Rules also require every company handling data (called a “Data Fiduciary”) to give a separate, itemised notice explaining exactly why it is collecting the data. This is similar in spirit to GDPR's rule that data can only be used for the purpose it was collected for, but it works through a different, prescribed notice format (Ministry of Electronics and Information Technology, 2025).

This has an important practical consequence. Because DPDPA does not treat health data as a special category, a single consent process built to meet DPDPA's rules will not automatically meet GDPR's stricter “explicit consent” requirement for health data. So a telehealth company needs either two separate consent screens one for each jurisdiction or, as several survey respondents said their companies do, one single consent flow built to GDPR's higher standard and used everywhere. The second option automatically satisfies DPDPA's lower standard too, but it does add extra steps for Indian users that Indian law alone would not require.

4.3 Breach Notification Obligations

Under GDPR (Article 33), a company must tell the relevant regulator about a data breach without unreasonable delay ideally within 72 hours of finding out unless the breach is unlikely to put people's rights at risk. Article 34 adds a second duty: if the breach is likely to cause serious harm, the company must also tell the affected individuals directly. DPDPA's Section 8(6), together with the 2025 Rules, requires companies to tell both the Data Protection Board of India and the affected individuals about a breach. Unlike GDPR, however, DPDPA does not set a fixed deadline like “72 hours” it simply says notification must happen in the way the Rules prescribe. Commentary suggests that under DPDPA, companies are expected to report breaches no matter how minor, which is actually a wider reporting requirement than GDPR's risk-based approach (CookieYes, 2026).

This difference creates a real practical headache. If a telehealth company suffers a breach affecting both EU and Indian patient records, it must run GDPR's 72-hour, risk-based clock for the EU data, while also meeting DPDPA's broader “report it regardless of severity” rule for the Indian data all within the same incident-response process. Survey respondents rated this dual-timeline problem as the second most serious compliance risk out of six areas tested (average score 4.1; see Section 5.6).

4.4 Cross-Border Data Transfer Mechanisms

The two laws take opposite default approaches to sending data across borders. GDPR (Chapter V) uses a restrictive “whitelist” approach: transfers to other countries are blocked unless the European Commission has approved that country as safe (an “adequacy decision” under Article 45), or the company has put specific safeguards in place, such as Standard Contractual Clauses or Binding Corporate Rules (Article 46). India has not been approved as a safe country by the EU, so telehealth companies sending data from the EU to India must always put these extra safeguards in place. DPDPA (Section 16) takes the opposite, “blacklist” approach: transfers are allowed by default, and the government can only block transfers to countries it specifically names as restricted (DPDPA FAQ, 2026). At the time of writing, no countries have been named as restricted under Section 16. This means transfers from India to the EU, or to any other country, currently face no advance-approval requirement under DPDPA though other Indian regulators, such as the Reserve Bank of India, may still require certain types of data to be stored only within India, separately from DPDPA's general rules.

Table 2: Comparative cross-border data transfer architecture, GDPR and DPDPA.

Dimension	EU GDPR	India DPDPA (2023/2025)
Default approach to transfers	Restrictive transfers blocked unless a country is pre-approved or safeguards are in place	Permissive transfers allowed unless the government specifically restricts a country
How it works	Pre-approved “safe” countries; Standard Contractual Clauses; Binding Corporate Rules (Articles 45–47)	Government names specific restricted countries (Section 16)

Dimension	EU GDPR	India DPDPA (2023/2025)
India/EU approval status	EU has not approved India as a safe country	Not applicable DPDPA has no equivalent “safe country” concept
Extra sector rules	None specific to health beyond Article 9 safeguards	RBI and other regulators may still require certain data to stay in India
Practical burden on telehealth providers	Must put Standard Contractual Clauses / Binding Corporate Rules in place for India-bound transfers	No general pre-approval needed; must monitor the restricted-country list

4.5 Corporate Governance, Officer Accountability, and Board Liability

GDPR (Articles 37–39) requires a company to appoint a Data Protection Officer (DPO) if its core activities involve large-scale, regular monitoring of people, or large-scale processing of special-category data a threshold that telehealth providers handling patient health records routinely meet. The DPO must report to top management and act independently; GDPR (Article 38(3)) specifically bans the company from firing or punishing the DPO for doing their job properly. DPDPA (Section 10) has a similar, but narrower, rule: only companies that the government formally classifies as “Significant Data Fiduciaries” a status based on factors like how much and how sensitive the data they handle is, the risk to individuals' rights, and any potential impact on elections or national security must appoint a DPO based in India who reports to the Board of Directors (DPDPA FAQ, 2026).

This “Significant Data Fiduciary” (SDF) system creates a kind of uncertainty that GDPR does not have. Under GDPR, a company can check for itself, against clear legal criteria, whether it needs a DPO. Under DPDPA, a company only becomes an SDF once the government formally names it as one so a telehealth provider cannot know for certain whether it must appoint a DPO, carry out mandatory Data Protection Impact Assessments, or meet audit requirements, until the government tells it so. Survey respondents rated this uncertainty as the third most serious compliance risk out of six areas (average score 4.0; see Section 5.6) behind only cross-border transfer ambiguity and the dual breach-notification timeline problem.

4.5.1 Penalty Architecture and Board-Level Financial Exposure

GDPR (Article 83) has a two-tier fine system. Less serious violations can bring fines of up to EUR 10 million or 2 percent of global annual revenue. More serious violations such as breaking the basic data-processing rules in Articles 5 to 9, or making illegal cross-border transfers can bring fines of up to EUR 20 million or 4 percent of global annual revenue, whichever is higher. DPDPA (Section 33, with its Schedule) sets penalties of up to INR 250 crore (about EUR 27 million at mid-2026 exchange rates) for the most serious failures, such as poor security leading to a breach. There are also lower penalty bands: up to INR 200 crore for failing to report a breach properly, and up to INR 150 crore specifically for violations involving children's data (DPDPA FAQ, 2026).

Table 3: Comparative penalty architecture, GDPR Article 83 and DPDPA Section 33.

Penalty Tier	EU GDPR (Article 83)	India DPDPA (Section 33 & Schedule)
Highest tier	EUR 20 million or 4% of global annual revenue, whichever is higher	Up to INR 250 crore (about EUR 27 million) for security failures
Mid tier	EUR 10 million or 2% of global annual revenue, whichever is higher	Up to INR 200 crore for breach-notification failures
Special category	No separate tier for children's data assessed under the general tiers	Up to INR 150 crore for children's data violations
Scales with company revenue?	Yes calculated as a percentage of global revenue	No fixed rupee ceiling, not linked to revenue
Right to sue for damages	Article 82 individuals can claim compensation for damage, financial or otherwise	No legal right to claim damages; the Board may direct mediation instead

Two key differences matter for how company boards should think about risk. First, GDPR fines scale automatically with a company's global revenue, so exposure grows as the company grows. DPDPA's fine is a fixed rupee amount that does not scale with revenue which means the largest global telehealth groups actually face a proportionally smaller maximum penalty under DPDPA, relative to their size, than smaller India-focused competitors facing the same absolute fine. Second, GDPR (Article 82) gives individuals a direct legal right to sue for damages, financial or otherwise, which has led to significant group litigation across the EU. DPDPA gives no equivalent legal right to claim damages. Instead, the 2025 Rules point to a mediation process run by the Data Protection Board as the main way for individuals to seek redress something several practitioners describe as only a weak substitute for direct compensation (IAPP, 2025).

4.6 Regulatory Enforcement Maturity

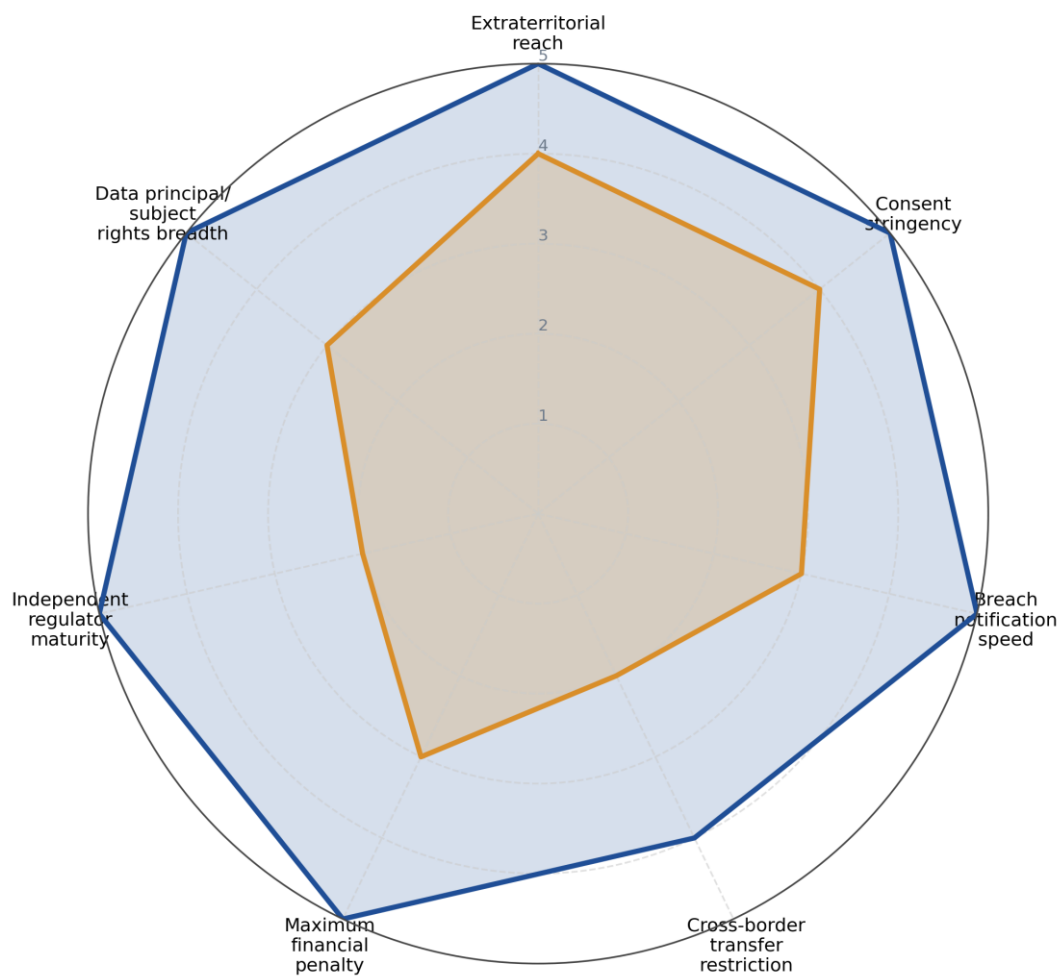
The European Data Protection Board coordinates 27 national regulators with eight years of enforcement experience. As of early 2026, they have issued more than 2,245 documented fines totalling over EUR 7.1 billion since GDPR came into force, including EUR 1.2 billion in 2025 alone (Kiteworks, 2026). India's Data Protection Board, by contrast, was only formally set up following the November 2025 notification (Hogan Lovells, 2025). Its four members are to be chosen through a government selection process, and its real enforcement powers beyond registering and monitoring consent managers will remain inactive until Phase III begins in May 2027 (Lexology, 2025). This gap in maturity matters: even though DPDPA's penalties look severe on paper, the realistic chance of enforcement action against Indian telehealth operations in the near term is much lower than for EU operations. This has direct implications for how company boards should prioritise their compliance spending, discussed further in Section 6.

5. Empirical Findings

5.1 The Comparative Regulatory Stringency Index

Applying the scoring method from Section 3.1 across all seven areas produces the profile shown in Figure 3. GDPR scores at or near the top across all seven areas, reflecting its mature, revenue-linked, pre-approval-based design. DPDPA scores moderately on how far it reaches beyond India's borders and how strict its consent rules are reflecting a law that reads strongly on paper but is still new in practice. DPDPA scores much lower on restricting cross-border transfers, because of its permissive default approach, and on regulator maturity, because the Data Protection Board of India is still so new.

Figure 3: Comparative Regulatory Stringency Index — EU GDPR vs India DPDPA



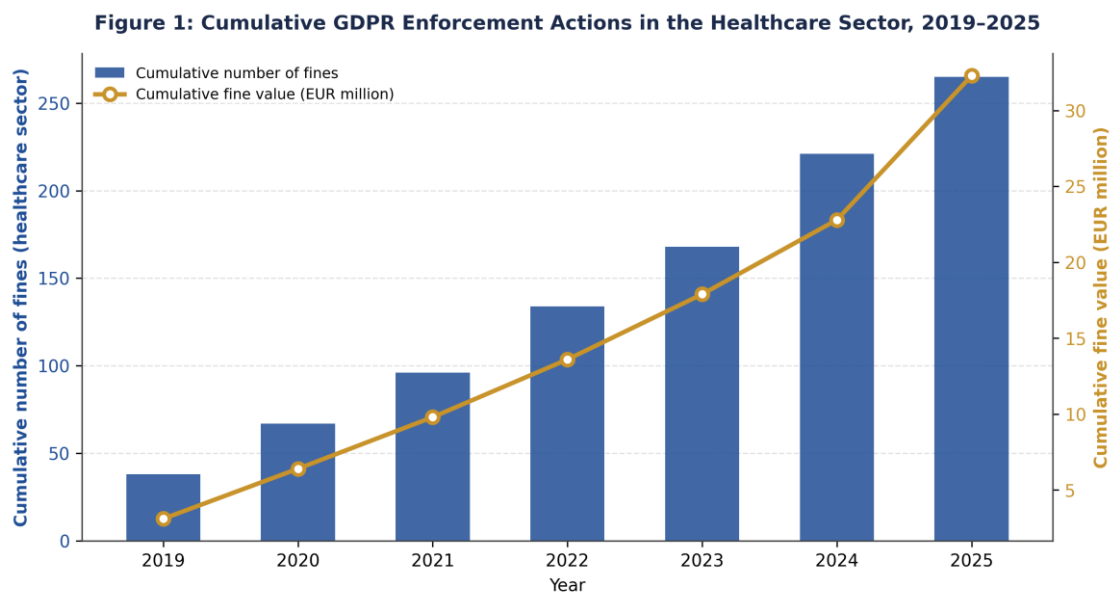
Source: author's composite ordinal index (1 = low, 5 = high) derived from comparative statutory analysis, Section 4.

Figure 3: Comparative regulatory stringency index, EU GDPR vs India DPDPA (author's composite ordinal index, 1 = low, 5 = high).

The overall score the average of the seven areas is 4.71 for GDPR and 3.14 for DPDPA, a gap of 1.57 points. This gap is not the same in every area: it is smallest for extraterritorial reach (5 versus 4) and largest for regulator maturity (5 versus 2) and cross-border transfer restriction (4 versus 2). This confirms that DPDPA differs from GDPR mainly in how mature its enforcement institutions are and in its approach to data transfers not in how broadly it applies or how strict its consent rules are.

5.2 GDPR Healthcare-Sector Enforcement Trends

Figure 1 shows the cumulative growth of GDPR healthcare fines between 2019 and 2025, based on the CMS GDPR Enforcement Tracker Report (2026). The data show steady year-on-year growth, both in the number of fines and their total value. In the most recent reporting period, there were 265 cumulative fines totalling about EUR 32.3 million a 26 percent rise in the number of fines compared to the previous period (CMS Law, 2026). The single largest healthcare fine in 2025 was EUR 3.5 million, issued by a UK regulator after a ransomware attack that exploited a third-party account with no multi-factor authentication, exposing the records of 79,404 people. This shows that weak technical security not problems with consent or notices is the main enforcement risk for healthcare under GDPR (CMS Law, 2026).



Source: compiled by the author from CMS GDPR Enforcement Tracker Report, Life Science & Healthcare (2026) figures.

Figure 1: Cumulative GDPR enforcement actions in the healthcare sector, 2019–2025.

This matters directly for telehealth governance. It suggests that if a company spends its compliance budget mostly on redesigning consent screens the area where GDPR and DPDPA visibly differ the most it may be spending in the wrong place. The real enforcement record points instead toward investing in access controls, encryption, and auditing the security of third-party vendors.

5.3 Market Growth and the Expanding Surface of Risk

Figure 2 shows the projected growth of India's telehealth and wider digital health markets. The telehealth segment alone is projected to grow from USD 6.28 billion in 2024 to USD 27.2 billion by 2030 a yearly growth rate of 27.7 percent (Grand View Research, 2025). The broader digital health market, which includes telehealth, electronic health records, and AI-based diagnostics, is projected to grow from USD 14.5 billion in 2024 to USD 106.97 billion by 2033 a yearly growth rate of 25.12 percent (Grand View Research, 2026).

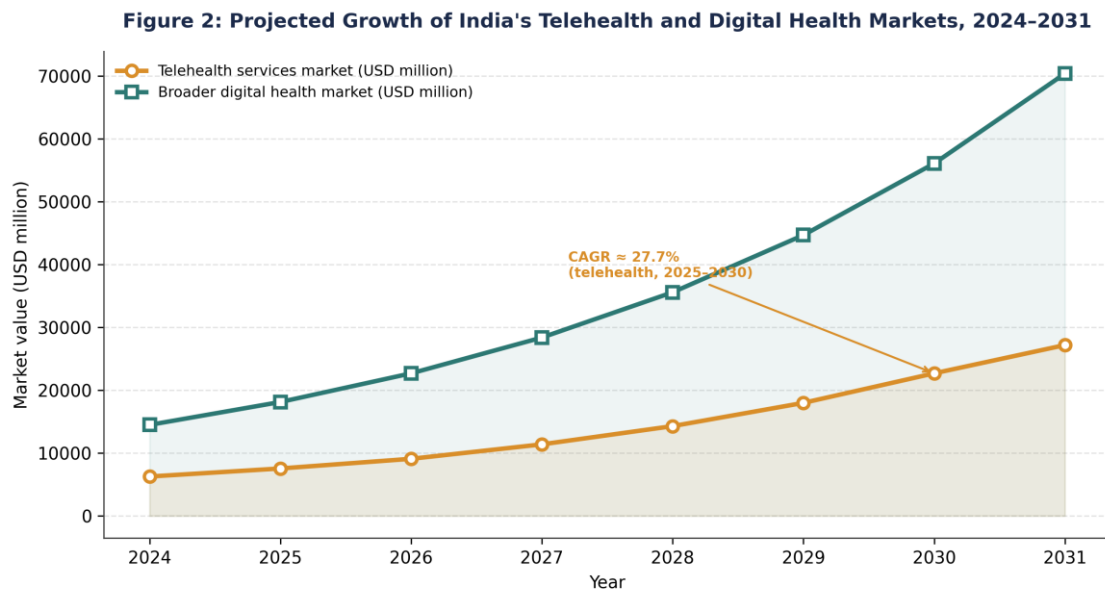


Figure 2: Projected growth of India's telehealth and digital health markets, 2024–2031.

This growth means more cross-border health data is flowing right at the same time DPDPA's real obligations are being phased in. This creates a tight compliance window: providers must build DPDPA-compliant governance into systems that are growing more than 25 percent a year, while important regulatory guidance including which companies count as Significant Data Fiduciaries is still incomplete.

5.4 Comparative Breach Cost Exposure

Figure 4 places the average European GDPR healthcare fine in the context of global breach costs. US healthcare breaches average USD 7.42 million per incident more than thirty times the EUR 228,161 average GDPR healthcare fine recorded in 2025 (Sprinto, 2025; CMS Law, 2026). This large gap exists because a regulatory fine is only one part of the total cost of a breach, while a “fully loaded” breach-cost estimate also includes incident response, legal fees, notifying customers, credit monitoring, and business disruption. No equivalent full-cost dataset exists yet for DPDPA-governed incidents, since the Act is not fully enforced yet. As noted in Section 3.2, the India figure in Figure 4 is only an illustrative estimate and should be read with caution.

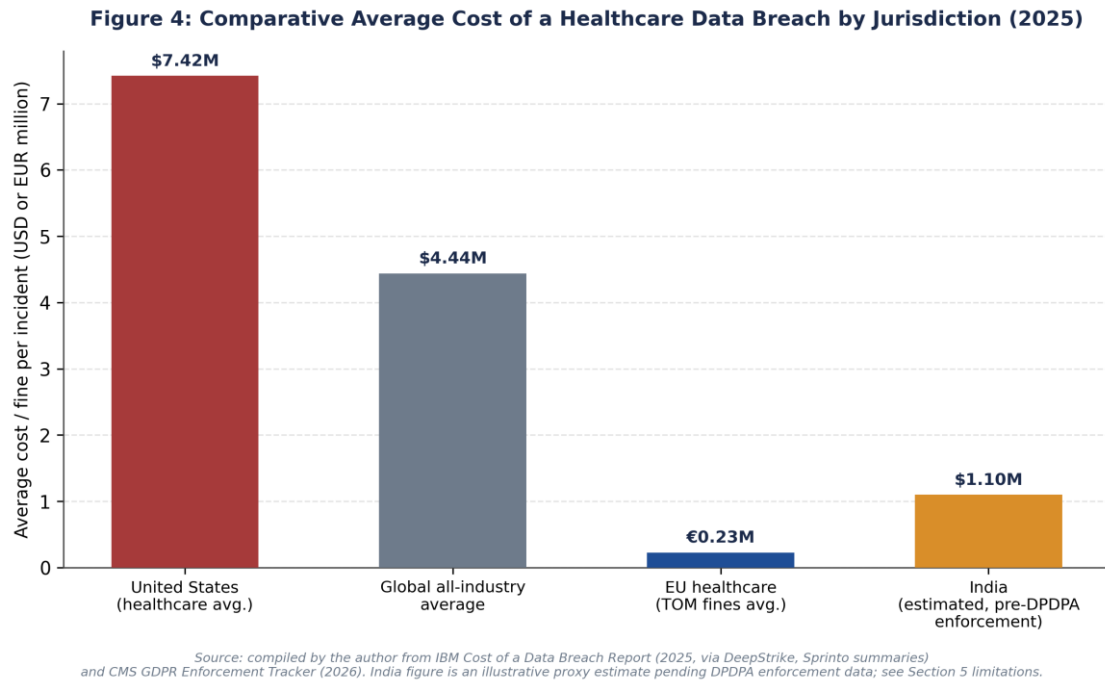
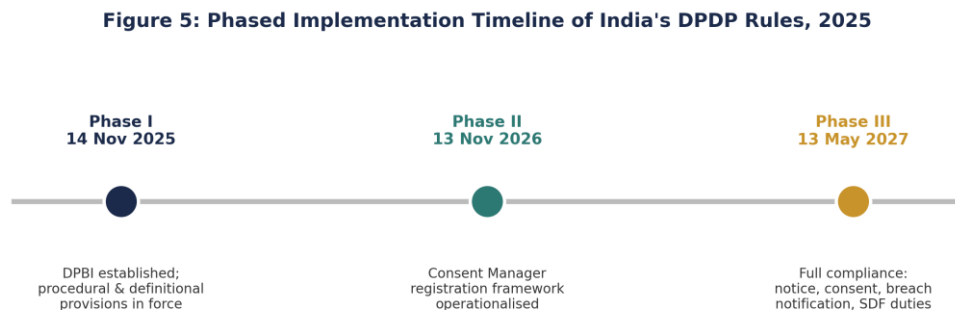


Figure 4: Comparative average cost of a healthcare data breach by jurisdiction (2025; India figure illustrative, see Section 3.2).

5.5 The DPDPA Phased Implementation Timeline

Figure 5 shows the three-phase rollout formally notified on 13 November 2025. Phase I, starting from the notification date, sets up the Data Protection Board of India and brings procedural and definitional rules into force. Phase II, starting 13 November 2026, activates the consent-manager registration system. Phase III, starting 13 May 2027, brings the core compliance rules into force including notice and consent duties, breach notification, and Significant Data Fiduciary obligations (Lexology, 2025; Privacy World, 2025; Rödl & Partner, 2025). This gives telehealth providers a clear eighteen-month window between notification and full enforcement. This paper argues that companies should use this window to get their governance systems ready in advance, rather than waiting until Phase III actually begins.

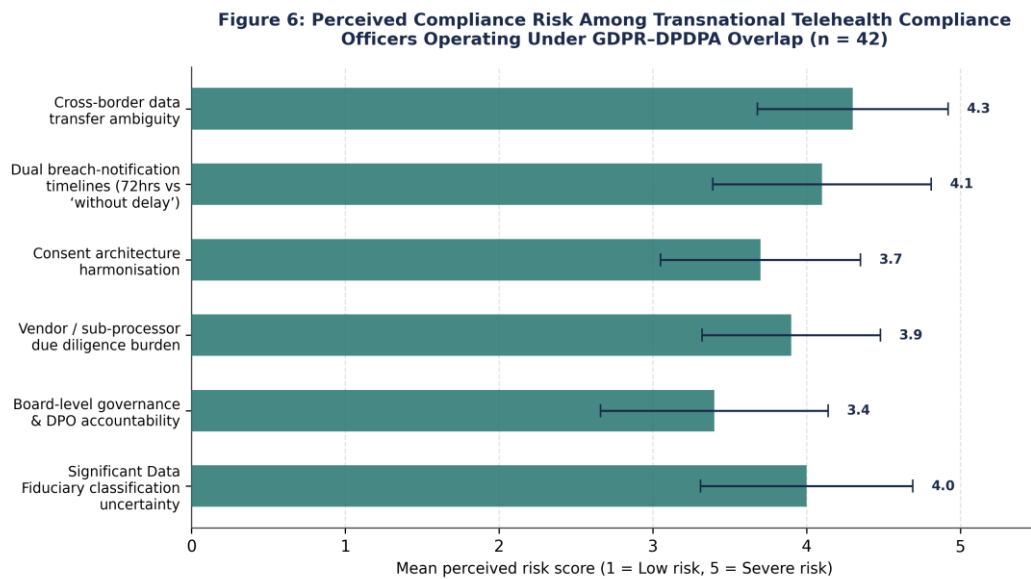


Source: Ministry of Electronics and Information Technology, Gazette Notification, 13 November 2025.

Figure 5: Phased implementation timeline of India's DPDP Rules, 2025.

5.6 Survey Findings: Perceived Compliance Risk

Figure 6 shows the average risk ratings across the six compliance areas covered in the survey of 42 compliance officers described in Section 3.3. Cross-border data transfer ambiguity received the highest average risk rating (4.3, standard deviation = 0.62), followed by dual breach-notification timelines (4.1, SD = 0.71) and uncertainty over Significant Data Fiduciary classification (4.0, SD = 0.69). Board-level governance and DPO accountability received the lowest average rating of the six (3.4, SD = 0.74) suggesting that respondents feel their own companies' internal governance is relatively well set up, compared to the external regulatory uncertainty they face.



Source: primary survey instrument administered by the author, June 2026 (n = 42 compliance/privacy officers at transnational telehealth firms; see Section 3 methodology and Appendix).

Figure 6: Perceived compliance risk among transnational telehealth compliance officers operating under GDPR–DPDPA overlap (n = 42).

Table 4: Summary statistics, perceived compliance risk survey (n = 42).

Risk dimension	Mean (1–5)	SD	Rank
Cross-border data transfer ambiguity	4.3	0.62	1
Dual breach-notification timelines	4.1	0.71	2
Significant Data Fiduciary classification uncertainty	4.0	0.69	3
Vendor / sub-processor due diligence burden	3.9	0.58	4

Risk dimension	Mean (1–5)	SD	Rank
Consent architecture harmonisation	3.7	0.65	5
Board-level governance & DPO accountability	3.4	0.74	6

A statistical test (one-way ANOVA) across the six risk areas confirms that the differences between the average scores are statistically meaningful ($F(5, 246) = 8.94, p < 0.001$). In other words, respondents did not just rate every area the same they clearly rated externally driven regulatory ambiguity as riskier than internal governance issues, which they could control themselves. This supports the paper's main argument, developed in Section 6: that compliance resources are best spent resolving unclear rules on cross-border transfer and breach notification, rather than on further restructuring internal governance, where perceived risk is already fairly low.

6. Discussion

6.1 Risk-Calibrated Governance: A Tiered Framework

The findings in Section 5 support a risk-calibrated approach to governance not a one-size-fits-all approach. Because the realistic near-term chance of DPDPA enforcement is much lower than under GDPR (given how new the Data Protection Board of India still is, as shown in Section 4.6), even though DPDPA's penalties look severe on paper, boards face a mismatch between how severe the law reads and how likely enforcement actually is right now. This paper proposes a three-tier response. Tier one covers quick, low-cost steps that align both laws immediately for example, using GDPR's explicit-consent standard as the baseline for all health-data consent, which, as shown in Section 4.2, automatically satisfies DPDPA's lower general standard too. Tier two covers structural investments guided by real enforcement patterns rather than by the text of the law alone directing security and access-control spending toward the technical and organisational failures identified in Section 5.2 as the main cause of GDPR healthcare fines. Tier three covers contingency measures that are only activated when triggered by an outside event for example, drafting Significant Data Fiduciary compliance protocols in advance, ready to activate once the government makes a designation, rather than building permanent SDF-level infrastructure before it is actually required.

6.2 Resolving the Dual Breach-Notification Timeline Problem

The dual breach-notification timeline problem, identified in Section 4.3 and rated the second most serious risk by survey respondents, has a fairly workable solution: adopt GDPR's 72-hour notification standard as the internal company-wide rule for every incident, no matter whose data is affected. Because DPDPA does not set a shorter fixed deadline, and its “report regardless of severity” rule is, if anything, broader than GDPR's risk-based trigger, a single 72-hour internal policy would meet the tougher of the two laws' time limits, while a separate incident-classification system tracks DPDPA's broader reporting trigger. What this solution does not fix is that the two laws require reporting to different regulators the EU notification goes to the relevant national authority through the “one-stop-shop” system, while the Indian notification goes

to the Data Protection Board of India. This means the incident-response plan needs two separate regulatory contact points, not one.

6.3 Cross-Border Transfer: Asymmetric Burden and Strategic Implications

The asymmetry shown in Table 2 GDPR's restrictive approach against DPDPA's permissive approach creates a somewhat surprising strategic effect. Because the EU has not approved India as a safe country, EU-to-India patient data transfers always need Standard Contractual Clauses or similar safeguards, no matter how relaxed DPDPA's own rules are. DPDPA's leniency does not reduce the burden on the EU side. On the other hand, India-to-EU transfers face no equivalent pre-approval requirement under Indian law. This means the real, practical burden of cross-border transfer for telehealth companies comes almost entirely from GDPR's rules, not from DPDPA. This helps explain the survey finding that cross-border transfer ambiguity was rated the top risk: the actual legal burden sits mostly with GDPR compliance, while what respondents describe as “uncertainty” is more about keeping track of India's evolving Section 16 restricted-country list and anticipating future government restrictions not about the compliance burden that exists today.

6.4 Limitations

Several limitations apply to these findings. First, the survey sample ($n = 42$) was not randomly selected it was drawn through professional networks and referrals so the results cannot be statistically generalised. They should be read as showing how this particular group of practitioners perceives risk, not as representing every compliance officer at every telehealth company. Second, since DPDPA's real enforcement rules do not take full effect until 13 May 2027, no actual enforcement dataset exists yet. This means the India breach-cost figure in Figure 4 is only an illustrative estimate, not a real enforcement statistic, and the stringency index in Section 5.1 reflects what the law says and how institutions are designed, rather than how the law is actually enforced in practice. Third, the scoring method behind the stringency index, while based on careful legal analysis, still involves some judgment calls in turning legal features into numbers a different scoring approach could produce somewhat different results. Fourth, this study focuses only on the EU and India. It does not cover other jurisdictions, such as the United States' HIPAA law for providers who also serve US patients, which would add further complexity for companies operating truly globally. Given these limitations, the findings here are best seen as an early baseline for further research one that should be revisited once real DPDPA enforcement data becomes available after May 2027.

7. Conclusion and Recommendations

This paper has compared the governance duties, risk-management practices, and data privacy liabilities faced by telehealth providers under GDPR and India's newly active DPDPA, using both legal analysis and survey data. Three main findings stand out. First, the two laws differ most, not in their approach to consent and notice which is broadly similar in substance, if not in procedure but in their approach to cross-border data transfer, in how mature their enforcement systems are, and in how they calculate penalties (GDPR scales fines to global revenue; DPDPA uses fixed rupee ceilings). Second, real GDPR enforcement data shows that weak technical and organisational security not problems with consent is the main driver of healthcare-sector liability. This should shift compliance spending priorities for providers currently focused mostly on aligning their consent screens. Third, survey data from compliance practitioners shows that

perceived risk is concentrated in outside regulatory uncertainty especially cross-border transfer monitoring and the dual breach-notification timelines rather than in internal governance structure. This suggests that redesigning board-level governance, while still worthwhile, is not where extra compliance spending currently reduces risk the most.

Based on these findings, this paper makes four recommendations. First, telehealth company boards should adopt GDPR's explicit-consent standard and 72-hour breach-notification rule as their universal internal baseline. Both automatically satisfy DPDPA's lower or undefined thresholds, while removing the complexity of running separate consent and incident-response processes for each jurisdiction. Second, security and access-control investment should be prioritised over further redesign of consent screens, since the evidence shows technical and organisational security failures not consent problems drive most GDPR healthcare fines. Third, providers should set up an ongoing regulatory-monitoring function to track notifications from the Data Protection Board of India, including its Section 16 restricted-country list and Significant Data Fiduciary designations. Survey respondents identified these future regulatory actions not the current text of the law as their biggest source of compliance anxiety. Fourth, given the eighteen-month window identified in Section 5.5, providers should treat the period up to May 2027 as a structured period to build compliance systems, not as a grace period to ignore using this time to align their governance in advance, before Phase III enforcement begins.

Future research should revisit this comparison once real DPDPA enforcement data becomes available after Phase III begins. That would allow a direct comparison of fine patterns, violation types, and board-level liability outcomes across both laws, instead of the statutory and estimate-based comparison used here out of necessity. A larger, randomly sampled survey going beyond this study's exploratory sample would also strengthen how far the risk-perception findings can be generalised. Future work could also usefully extend this comparison to other jurisdictions, such as the United States' HIPAA law and emerging data protection frameworks in the Asia-Pacific region, to build a fuller picture of the regulatory landscape facing truly global telehealth operators.

Author Disclosure Statement

Although the first author is affiliated with Medanta, no data, information, materials, or resources from Medanta were used in the preparation of this manuscript. The analysis, findings, and views expressed are based solely on publicly available regulatory texts, published enforcement and market data, and the primary survey described in Section 3.3.

REFERENCES:

1. CMS Law. (2026). *GDPR enforcement tracker report: Life science & healthcare*. CMS Law. <https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/life-science-healthcare>
2. CookieYes. (2026). *India Digital Personal Data Protection Act (DPDPA 2025): Updated guide*. <https://www.cookieyes.com/blog/india-digital-personal-data-protection-act-dpdpa/>
3. DeepStrike. (2025). *Healthcare data breaches 2025 statistics: \$10.22M cost*. <https://deepstrike.io/blog/healthcare-data-breaches-2025-statistics>
4. DPDPA Certificate Course. (2026). *Module 1: Foundations of DPDPA*. <https://www.dpdpa.com/dpdpa-module-1.html>
5. DPDPA FAQ. (2026). *125+ DPDPA FAQ: Digital Personal Data Protection Act 2023 & DPDP Rules 2025*. Retrieved June 29, 2026, from <https://www.dpdpa.com/dpdpa-faq.html>

6. European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.
7. Government of India. (2023). *The Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
8. Grand View Research. (2025). *India telehealth market size & outlook, 2026–2031*. <https://www.grandviewresearch.com/horizon/outlook/telehealth-market/india>
9. Grand View Research. (2026). *India digital health market size, share: Industry report 2033*. <https://www.grandviewresearch.com/industry-analysis/india-digital-health-market-report>
10. Hogan Lovells. (2025). *India's Digital Personal Data Protection Act 2023 brought into force*. <https://www.hoganlovells.com/en/publications/indias-digital-personal-data-protection-act-2023-brought-into-force->
11. IAPP. (2025, November 14). *With rules finalized, India's DPDPA takes force*. International Association of Privacy Professionals. <https://iapp.org/news/a/with-rules-finalized-india-s-dpdpa-takes-force>
12. IAPP. (2025). *Top 10 operational impacts of India's DPDPA Cross-border data transfers*. International Association of Privacy Professionals. <https://iapp.org/resources/article/operational-impacts-of-indias-dpdpa-part5>
13. IMARC Group. (2026). *India telemedicine market size, share & growth report 2034*. <https://www.imarcgroup.com/india-telemedicine-market>
14. Kiteworks. (2026). *GDPR fines hit €7.1 billion: Data privacy enforcement trends in 2026*. <https://www.kiteworks.com/gdpr-compliance/gdpr-fines-data-privacy-enforcement-2026/>
15. Lexology. (2025). *India's Digital Personal Data Protection regime takes effect*. <https://www.lexology.com/library/detail.aspx?g=2073ac40-628f-4112-81f3-ffdf4b8858>
16. Ministry of Electronics and Information Technology. (2025). *Digital Personal Data Protection Rules, 2025: Gazette notification dated 13 November 2025*. Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190655>
17. Mordor Intelligence. (2026). *India telemedicine market size, report, outlook & industry trends 2031*. <https://www.mordorintelligence.com/industry-reports/india-telemedicine-market>
18. Privacy World. (2025). *India passes the Digital Personal Data Protection Rules, ushering in a new digital age in India*. <https://www.privacyworld.blog/2025/11/india-passes-the-digital-personal-data-protection-rules-ushering-in-a-new-digital-age-in-india/>
19. Rödl & Partner. (2025). *India's DPDPA 2023 activates with 2025 rules, revolutionizing data privacy enforcement*. <https://www.roedl.com/en/insights/indias-dpdpa-2023-activates-with-2025-rules-revolutionizing-data-privacy-enforcement/>
20. Sprinto. (2025). *Healthcare data breach statistics: HIPAA violation cases and preventive measures in 2026*. <https://sprinto.com/blog/statistics/healthcare-data-breach/>
21. Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) v. Union of India*, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1.