Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

Cross-Border Healthcare Data Governance: Assessing India's Legal Framework in Light of the European Health Data Space

Faisal Yaseen[1], Fahaad[2]

[1]Assistant Manager, Medanta Hospital, [2]Advocate, Delhi

Abstract:
This paper examines India's regulatory architecture for cross-border healthcare data flows under the Digital Personal Data Protection Act, 2023 against the European Union's newly operational European Health Data Space Regulation (EU) 2025/327. It argues that India's jurisdiction-agnostic, "negative-list" approach to data export, combined with the DPDP Act's abandonment of a distinct sensitive-data category, leaves health information without the tiered safeguards that both the erstwhile Sensitive Personal Data or Information Rules and the GDPR-EHDS regime supply. Employing doctrinal methodology, the analysis of constitutional text, statute, and delegated legislation the paper identifies three structural divergences between the regimes and proposes a sector-specific health-data governance instrument for India.

Keywords: Cross-Border Healthcare Data, Health Data Governance, Digital Personal Data Protection Act, 2023, European Health Data Space (EHDS), Cross-Border Data Transfers.

I. Introduction

Health data occupies a paradoxical position in data protection law: it is simultaneously among the most consequential categories of personal information for individual dignity and among the most valuable for public health research, insurance underwriting, and biomedical innovation. The COVID-19 pandemic accelerated the digitisation of health records worldwide, and India's Ayushman Bharat Digital Mission ("ABDM"), together with the European Union's European Health Data Space ("EHDS"), represent two of the most ambitious contemporary efforts to build interoperable digital health infrastructures. Yet the two jurisdictions have arrived at markedly different governance philosophies. The EHDS, given legal form by Regulation (EU) 2025/327,[1] creates a bespoke sectoral regime layered atop the General Data Protection Regulation ("GDPR"), complete with Health Data Access Bodies, an opt-out mechanism for secondary use, and a dedicated cross-border infrastructure, HealthData@EU. India, by contrast, regulates health data through the horizontal, sensitivity-agnostic Digital Personal Data Protection Act, 2023 ("DPDP Act"),

[1]Regulation 2025/327, of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and Amending Directive 2011/24/EU and Regulation 2024/2847, 2025 O.J. (L, 2025/327) [hereinafter EHDS Regulation].

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

operationalised by the Digital Personal Data Protection Rules, 2025 ("DPDP Rules"), which entered into force in a phased manner beginning in November 2025.[2] This paper undertakes a doctrinal comparison of the two frameworks to assess whether India's law adequately governs the cross-border movement of health data, and to identify the reforms necessary to align India with emerging international norms of health-data-specific protection.

II. Constitutional and Statutory Foundations in India

The Indian framework begins not in statute but in constitutional adjudication. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[3] a nine-judge bench of the Supreme Court held that privacy, including informational privacy, is intrinsic to the right to life and personal liberty under Article 21 of the Constitution, and articulated a three-fold test of legality, legitimate state aim, and proportionality for any intrusion. *Puttaswamy* furnished the constitutional predicate for a comprehensive data protection statute and was repeatedly invoked during the legislative deliberations preceding the DPDP Act.

The DPDP Act, enacted on 11 August 2023 and brought into force in a phased manner through notifications issued on 13–14 November 2025,[4] is India's first comprehensive horizontal data protection law. It replaced Section 43A of the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"),[5] which had defined "sensitive personal data or information" to expressly include physical, physiological and mental health condition, medical records and history, and biometric information, and had prescribed heightened consent and security obligations for such data. Significantly, the DPDP Act abandons this tiered structure altogether: it applies a uniform standard of consent or "legitimate use" to all "personal data" without distinguishing health information for heightened statutory protection, a departure that commentators have criticised as increasing the vulnerability of data principals whose medical information is processed.[6]

[2]Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023) [hereinafter DPDP Act]; Digital Personal Data Protection Rules, 2025, G.S.R. 843(E) (Nov. 13, 2025) (India) [hereinafter DPDP Rules]; see also Shardul Amarchand Mangaldas & Co, Enforcement of the DPDP Act and Notification of the DPDP Rules (Nov. 27, 2025), https://www.amsshardul.com/insight/enforcement-of-the-dpdp-act-and-notification-of-the-dpdp-rules/.

[3]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 3, 325 (India) (recognizing informational privacy as intrinsic to Article 21 of the Constitution and articulating a three-fold test of legality, legitimate aim, and proportionality for any state intrusion).

[4]Shardul Amarchand Mangaldas & Co, supra note 3 (noting the Ministry of Electronics and Information Technology published notifications on 13-14 November 2025 bringing the DPDP Act and DPDP Rules into force on a staggered timeline culminating on 14 May 2027).

[5]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), r. 3 (India) (defining "sensitive personal data or information" to include, inter alia, physical, physiological and mental health condition, medical records and history, and biometric information); Information Technology Act, No. 21 of 2000, § 43A, India Code (2000).

[6]Removing the Category of 'Sensitive' Personal Data under the DPDPA: Heightening Data Principal Vulnerability, Indian J.L. & Tech. Blog (2026), https://forum.nls.ac.in/ijlt-blog-post/removing-the-category-of-sensitive-personal-data-under-the-dpdpa-heightening-data-principal-vulnerability/.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

The Act's principal cross-border provision, Section 16,[7] adopts what is commonly described as a "negative list" or "blacklist" model: transfer of personal data outside India is permitted to any country or territory except one that the Central Government expressly restricts by notification; as of the date of this paper, no such notification has issued, rendering the default position one of largely unrestricted transferability.[8] The DPDP Rules qualify this only for Significant Data Fiduciaries ("SDFs"), whom Rule 13(4) prohibits from transferring specified categories of traffic data relating to the flow of personal information outside Indian territory, and permit stricter sector-specific localisation laws to prevail over the DPDP Act's default.[9]

Parallel to the DPDP framework, the Health Data Management Policy of the ABDM, issued by the National Health Authority,[10] imposes a consent-based architecture for health information exchanged through the ABDM's federated infrastructure, including the Ayushman Bharat Health Account. The Policy predates and has not been formally harmonised with the DPDP Act, creating an uncodified, policy-level layer of protection that lacks the statutory force of the EHDS's access-governance provisions discussed below.

III. The European Health Data Space: A Sectoral Model

The European Union's approach begins from the opposite premise. Article 9 of the GDPR[11] designates "data concerning health" a "special category" of personal data whose processing is prohibited by default, subject to enumerated derogations such as explicit consent, provision of healthcare, or public interest in public health each requiring "suitable and specific measures" to safeguard the data subject. Building on this foundation, the European Parliament and Council adopted Regulation (EU) 2025/327 establishing the EHDS, published in the Official Journal on 5 March 2025 and entered into force on 26 March 2025, following a legislative process that began with the Commission's proposal of 3 May 2022.[12]

The EHDS pursues two distinct regulatory objects. For "primary use," it grants natural persons enhanced rights to access, port, and rectify their own electronic health data across Member State borders, harmonised through common European electronic health record exchange formats. For "secondary use," it establishes

[7]DPDP Act, supra note 3, § 16.

[8]See Cross-Border Data Transfers Under India's Digital Personal Data Protection Act, 2023: A Compliance Guide for Global Businesses, Lexology (2026), https://www.lexology.com/library/detail.aspx?g=ce5725ab-e3c8-4070-855d-0519e36dead9; Taxmann, Cross-Border Data Transfers Under the DPDP Act 2023 (May 4, 2025), https://www.taxmann.com/post/blog/cross-border-data-transfers-under-the-dpdp-act/.

[9]DPDP Rules, supra note 3, r. 13(4); S.S. Rana & Co., MeitY Notifies Final Digital Personal Data Protection Rules 2025 (Apr. 3, 2026), https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/.

[10]Ministry of Health & Family Welfare, National Health Authority, Health Data Management Policy (Ayushman Bharat Digital Mission) (2022), https://abdm.gov.in/hdmp-comments-view.

[11]Regulation 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 (General Data Protection Regulation), art. 9, 2016 O.J. (L 119) 1 [hereinafter GDPR].

[12]EHDS Regulation, supra note 2; Eva Schnitzler, European Union: New Regulation Establishes the European Health Data Space for Exchange of Health Records, Libr. of Cong., Global Legal Monitor (May 5, 2025), https://www.loc.gov/item/global-legal-monitor/2025-05-05/european-union-new-regulation-establishes-the-european-health-data-space-for-exchange-of-health-records/ (noting publication in the Official Journal on 5 March 2025 and entry into force on 26 March 2025, following the Commission's proposal of 3 May 2022).

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

a first-of-its-kind mandatory access regime: researchers, public bodies, and industry may apply to national Health Data Access Bodies for pseudonymised or anonymised health data for research, innovation, and policy-making, while natural persons generally retain a right to object rather than a requirement of fresh consent for each secondary use.[13] Cross-border secondary use is to be channelled through HealthData@EU, an interoperable platform for which the Commission must adopt implementing technical specifications, and for which each Member State must designate a national contact point serving as an organisational and technical gateway.[14] The Regulation's compliance architecture is keyed to staggered milestones, with implementing acts due by March 2027, the exchange of priority primary-use data categories and most secondary-use rules applying from March 2029, and a second tranche of primary-use categories, including medical imaging and laboratory results, from March 2031.[15] Throughout, the EHDS preserves the underlying GDPR lawful bases and data-subject rights, layering its access-governance machinery on top of, rather than in substitution for, general data protection law.

IV. Comparative Analysis: Structural Divergences

Three divergences are of particular doctrinal significance. **First, categorical treatment.** The EU treats health data as inherently high-risk, prohibiting its processing absent an enumerated lawful ground, whereas the DPDP Act, having deliberately excised the sensitive-data category present in both the SPDI Rules and the 2018 Justice B.N. Srikrishna Committee draft, subjects health data to the same baseline consent-or-legitimate-use test applicable to an email address or purchase history. The consequence is that an Indian data fiduciary processing genomic or psychiatric records faces no statutorily heightened obligation of the kind Article 9 GDPR imposes, though the DPDP Act does permit the government to designate high-volume processors of sensitive data as SDFs subject to additional obligations, including data protection impact assessments.[16]

Second, the consent architecture for secondary use diverges sharply. The EHDS installs a right-to-object default for research and policy access to health data, administered through independent Health Data Access Bodies that vet applications and issue permits, institutionalising a distinct trust intermediary between data holders and secondary users. India has no statutory equivalent; the ABDM's consent-manager framework governs primary clinical-data exchange but does not extend to a comparable secondary-use permitting regime, leaving reuse of health data for research largely to sectoral guidelines, institutional ethics committees, and bilateral contractual arrangements outside the DPDP Act's text.[17]

Third, and most directly relevant to cross-border governance, the two regimes adopt inverse default rules for data export. The GDPR conditions third-country transfer on an adequacy finding, standard

[13]EHDS Regulation, supra note 2, Recital 1, art. 1; Global Legal Monitor, supra note 13.
[14]EHDS Regulation, supra note 2, Recital 80, art. 75; Global Legal Monitor, supra note 13.
[15]European Health Data Space, Deadlines, Milestones (2026), https://www.european-health-data-space.com/ (last visited July 20, 2026).
[16]DPDP Act, supra note 3, § 10 (significant data fiduciary obligations).
[17]AMLEGALS, Health Data and the DPDP Act: A Practical Guide (Nov. 20, 2025), https://amlegals.com/health-data-and-the-dpdp-act-a-practical-guide/ (describing the DPDP Act's "risk-based approach" in the absence of a statutory "sensitive personal data" category).

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

contractual clauses, or a comparable safeguard, placing the burden on the exporter to justify transfer.[18] Section 16 of the DPDP Act inverts this logic: transfer is permitted unless the destination is affirmatively blacklisted, placing the burden on the state to identify unsafe jurisdictions rather than on the exporter to establish safety.[19] For ordinary personal data this may be a defensible calibration of India's economic interest in outbound data flows, including business-process-outsourced medical transcription and diagnostic-imaging analytics; for health data specifically, the absence of any destination-sensitive assessment is a material governance gap when measured against the EHDS's safeguard requirements.

V. Cross-Border Implications and Gaps in the Indian Framework

These structural divergences generate concrete cross-border risks. Indian telemedicine platforms, diagnostic-imaging outsourcing firms, and clinical-research organisations increasingly transmit patient data to processors in the United States, the European Union, and elsewhere; under Section 16, such transfers require no destination-specific risk assessment so long as the recipient jurisdiction is not blacklisted, even though the same data, moving in the reverse direction, would be subject to the EU's adequacy or standard-contractual-clause requirements before it could lawfully reach an Indian processor. This asymmetry complicates reciprocal recognition: Indian entities seeking to receive research-grade health data from EHDS Health Data Access Bodies would need to satisfy EU adequacy or safeguard standards that the DPDP Act does not, on its own terms, guarantee, since India has articulated no equivalent categorical protection for health data against which an adequacy assessment could be benchmarked.

A second gap concerns localisation. Rule 13(4) restricts SDFs from exporting specified traffic data, but the criteria for designating an entity an SDF remain unnotified, leaving health-data processors uncertain whether ABDM-linked hospital networks, insurers, or diagnostic chains will fall within the stricter regime.The EHDS, by contrast, fixes obligations directly by reference to the nature of the data electronic health data rather than by a discretionary fiduciary-classification mechanism, yielding greater ex ante certainty for cross-border compliance planning.

VI. Recommendations

Three reforms would narrow the gap identified above. **First,** the Central Government, exercising rule-making power under the DPDP Act, should reintroduce a defined category of health or sensitive personal data carrying heightened consent, security, and impact-assessment obligations, restoring continuity with the SPDI Rules' definition while remedying that instrument's enforcement weaknesses. **Second,** India should consider a sectoral secondary-use permitting body, analogous to the EHDS's Health Data Access Bodies, to formalise research and policy access to ABDM-linked health data under codified, auditable criteria rather than ad hoc institutional consent. **Third,** Section 16 should be supplemented, for health data specifically, with a destination-sensitivity assessment or a requirement of contractual safeguards comparable to the GDPR's standard contractual clauses, which would both protect data principals and

[18]GDPR, supra note 12, arts. 44-49 (Chapter V, conditioning third-country transfer on an adequacy decision, appropriate safeguards such as standard contractual clauses, or a derogation).

[19]Taxmann, supra note 9.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 4, July-August 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i04.1477

position India favourably for a future EU adequacy-style determination facilitating two-way health-data research collaboration.

VII. Conclusion

India and the European Union have built parallel digital health infrastructures animated by a shared constitutional commitment to informational privacy, articulated in *Puttaswamy*[20] and in the GDPR's foundational recitals respectively. Yet at the level of statutory design, the EHDS's categorical, access-governed model and the DPDP Act's uniform, export-permissive model diverge sharply. As cross-border telemedicine, diagnostic outsourcing, and biomedical research intensify, India's failure to distinguish health data as a protected statutory category, and its residual reliance on a blacklist model for outbound transfer, leave an operative gap between the ambitions of the ABDM and the safeguards that international health-data governance increasingly demands. A doctrinally coherent path forward should draw on the EHDS not as a template for wholesale transplantation, but as a comparator against which India's next generation of health-data rules ought to be measured.

[20]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).