HEALTH DATA AND PRIVACY UNDER INDIA'S DATA PROTECTION REGIME: AN EXAMINATION OF THE ADEQUACY OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, FOR THE PROTECTION OF HEALTH DATA IN THE INDIAN HEALTHCARE SYSTEM

Gurveer Singh Dhindsa, LL.B. (Hons.), O.P. Jindal Global University,
Jindal Global Law School (2023–2026)

ABSTRACT

The Digital Personal Data Protection Act, 2023 ("DPDP Act") is India's first comprehensive statutory framework for the processing of digital personal data, built on consent, purpose limitation and accountability.[1] Unlike the draft bills that preceded it, however, the Act does not define or treat health data as a distinct, "sensitive" category requiring heightened protection. This paper examines the legal regime governing health data in India, tracing its evolution from Section 43A of the Information Technology Act, 2000[2] and the SPDI Rules, 2011,[3] through the unimplemented Digital Information Security in Healthcare Act and the Health Data Management Policy, to the DPDP Act and the Digital Personal Data Protection Rules, 2025. It argues that the Act's general, category-blind structure - read together with its exceptions and exemptions - leaves significant areas of health data under-protected, and proposes a set of reforms to reconcile patient privacy with public health objectives and the continued expansion of India's digital health ecosystem.

[1]Digital Personal Data Protection Act 2023.
[2]Information Technology Act 2000, s 43A.
[3]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

1. INTRODUCTION

In the last decade, digitisation has transformed healthcare delivery in India. Vast amounts of data are now generated, stored and shared electronically concerning people's bodies, diseases, treatments, and genetic makeup. The Ayushman Bharat Digital Mission ("ABDM") and the Ayushman Bharat Health Account ("ABHA") ecosystem aim to establish a digital health identifier for every citizen, connecting medical records across hospitals, clinics, laboratories and digital health applications.[4] This digital architecture offers continuity of care, administrative efficiency and public health surveillance benefits, but it also draws an unusually sensitive category of data into interoperable digital systems, creating commensurate risks of unauthorised access, secondary use, discrimination and large-scale data breaches.

Health information occupies a special place among categories of personal data. Where, for instance, an online user may have little concern about an advertiser mining their shopping or browsing history, health information reveals facts about a person's body, mind, ancestry, sexuality, disability and mortality that, if disclosed without consent, can cause social stigma, employment discrimination, denial of insurance coverage, reputational harm, and a broader chilling effect on people's willingness to seek medical care. Having recognised privacy as a fundamental right under Article 21 of the Constitution,[5] the Supreme Court of India identified informational privacy - including the privacy of medical records - as integral to human dignity and autonomy.[6] The statutory framework built to give effect to that constitutional guarantee now exists in the form of the Digital Personal Data Protection Act, 2023. The question this paper asks is whether that framework is adequate.

Before 2023, India had a fragmented and limited data-protection regime. The principal legislation - Section 43A of the Information Technology Act, 2000 and the Sensitive Personal Data or Information Rules, 2011 made under it[7] - applied only to body corporates, imposed only a non-contractual duty to maintain "reasonable security practices," and contained no general framework of rights, duties or institutional oversight. The Government of India recognised these limitations and, in 2017, constituted the Justice B.N. Srikrishna Committee,

[4]National Health Authority, Ayushman Bharat Digital Mission: Strategy Overview and ABHA (Ayushman Bharat Health Account) Documentation and Guidelines (Ministry of Health and Family Welfare).
[5]Constitution of India, art 21.
[6]*Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.*
[7]Information Technology Act 2000, s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

whose report formed the basis for the Personal Data Protection Bill, 2019, approved by the Union Cabinet in December 2019.[8] That Bill, and the Joint Parliamentary Committee that scrutinised it, retained the concept of "sensitive personal data" encompassing health, biometric and genetic data, subject to heightened obligations such as explicit consent and data protection impact assessments. The Digital Personal Data Protection Act, 2023, which received Presidential assent on 11 August 2023,[9] departs from this approach: it removes the distinction between "personal data" and "sensitive personal data" and applies a single, uniform set of obligations to all digital personal data, subject to a general regime of "certain legitimate uses" and exemptions that bear particularly on the healthcare sector.

2. RESEARCH QUESTIONS, OBJECTIVES AND METHODOLOGY

Whether the Digital Personal Data Protection Act, 2023, read together with its subordinate legislation and earlier sector-specific enactments, affords health data generated, stored and processed within the Indian healthcare system an appropriate and adequate legal-protection framework is the central inquiry of this research. This overarching question is broken down into four subsidiary research questions.

First, is the exclusion of health data as a distinct, "sensitive" category of personal data under the DPDP Act a normatively defensible policy choice, or does it constitute a structural weakness that leaves patients exposed to a higher risk of harm than they faced under the earlier draft data-protection bills and comparable foreign regimes?

Second, do the "certain legitimate uses" defined in Section 7 of the Act - including "medical emergencies," "epidemics and other threats to public health," and "the performance of State functions" - and the exemptions in Section 17[10] for State instrumentalities and for research and statistical purposes, satisfy the constitutional requirements of necessity and proportionality as applied to health data? And how do the DPDP Act and the DPDP Rules, 2025 interact with sector-specific instruments for digital health, such as the Health Data Management Policy under the ABDM, the Electronic Health Record Standards for India, 2016,

[8]Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, 2018).
[9]Digital Personal Data Protection Act 2023.
[10]Digital Personal Data Protection Act 2023, s 17.

and the never-enacted Digital Information Security in Healthcare Act?[11]

Third, what lessons can India draw from comparative data-protection regimes - particularly the "special categories" approach under the European Union's General Data Protection Regulation and the sectoral approach under the United States' Health Insurance Portability and Accountability Act - in reforming its own regime for health data?

Fourth, what legal, institutional and regulatory changes are needed to balance patient privacy, public health imperatives, and India's ongoing digital-health transformation, within the framework of the DPDP Act and its accompanying regulations?

Methodologically, this study adopts a doctrinal approach, drawing on the text of statutes and subordinate legislation, judicial decisions (in particular the Supreme Court's privacy jurisprudence), policy documents issued by the National Health Authority and the Ministry of Health and Family Welfare,[12] and authoritative secondary sources - including law-firm commentary and regulatory analyses published since the DPDP Rules were notified in November 2025. The analysis follows a textual and structural approach to the DPDP Act's provisions as they apply, directly or by implication, to health data, combined with a contextual examination of how those provisions interact with the ABDM ecosystem in practice. References to the European Union and the United States are not proposals for wholesale transplantation - both operate in constitutional, administrative and healthcare-financing contexts very different from India's - but are used to identify normative benchmarks against which the Indian framework can be assessed. This is not an empirical study: it does not survey patients or healthcare providers, and its conclusions are confined to an analysis of legal texts and documented practice.

3. FRAGMENTATION AND LIMITED PROTECTION IN THE PRE-DPDP LEGAL LANDSCAPE

The trajectory of health-data protection in India cannot be understood apart from the constitutional recognition of the right to privacy. In Justice K.S. Puttaswamy (Retd.) v Union

[11]Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, 110 Stat 1936 ('HIPAA'); Ministry of Health and Family Welfare, Electronic Health Record Standards for India (2016); National Health Authority, Health Data Management Policy (revised draft, April 2022).
[12]National Health Authority (n 4).

of India,[13] a nine-judge bench of the Supreme Court held that the right to privacy is integral to Article 21 of the Constitution - the right to life and personal liberty - and to the freedoms guaranteed by Part III more generally. The judgment matters for this paper because the privacy of medical information recurs throughout the concurring opinions as a paradigm case of informational privacy: information whose disclosure without consent causes dignitary harm, as with an individual's HIV status, mental-health history, or reproductive choices. The judgment thus supplied the normative impetus for a comprehensive data-protection law and signalled that any such law would need to address the heightened sensitivity of health data. It is against this constitutional backdrop that the subsequent legislative developments discussed below should be evaluated.

Before the DPDP Act, the principal legislation protecting personal data in India was Section 43A of the Information Technology Act, 2000, inserted by the Information Technology (Amendment) Act, 2008. Section 43A imposed civil liability on a "body corporate" possessing, dealing with or handling any "sensitive personal data or information" in a computer resource it owns, controls or operates, where negligence in implementing reasonable security practices caused wrongful loss or wrongful gain to any person. The Sensitive Personal Data or Information Rules, 2011, made under Section 43A, defined "sensitive personal data or information" to include passwords, financial information, physical and physiological health conditions, medical records and history, biometric information, and related categories - extending a degree of recognition to health information as sensitive.

This early regime, however, suffered from well-documented limitations so far as the healthcare sector was concerned. First, the SPDI Rules applied only to "body corporates," excluding public health authorities, government hospitals, and the many non-corporate bodies that handle the bulk of health data within India's public healthcare system. Second, the Rules created rights only in cases of wrongful loss or gain, rather than a general suite of data-principal rights - access, correction, portability, erasure and the like - and provided no institutional mechanism for oversight, investigation or enforcement beyond ordinary civil remedies. Third, the Rules permitted disclosure of sensitive personal data on the mere consent of the provider of information, without a purpose-limitation principle of the kind later found in comprehensive data-protection statutes, and without provisions tailored to research, health surveillance, or large-scale digital health initiatives of the kind the ABDM would develop a decade later.

[13] Justice K.S. Puttaswamy (Retd) v Union of India (n 6).

The result was a regime that recognised health data as sensitive in name, but was structurally unable to meet the scale and complexity of digital health-data processing that the Indian healthcare system would come to generate.[14]

4. THE DPDP ACT, 2023: ARCHITECTURE AND THE TREATMENT OF HEALTH DATA

4.1 General Architecture of the Act

The Digital Personal Data Protection Act, 2023 applies to the processing of digital personal data within India; to personal data collected in non-digital form in India and subsequently processed digitally; and, in some circumstances, to processing outside India where it is connected with offering goods or services to individuals within India. The Act is structured around the relationship between the "Data Fiduciary" - the entity determining the purpose and means of processing - and the "Data Principal", the individual to whom the data relates. Chapter II sets out the obligations of Data Fiduciaries, including the requirement that data be processed only for a lawful purpose for which the Data Principal has given consent, or which falls within the "certain legitimate uses" specified in Section 7.[15] The principles of valid consent - free, specific, informed, unconditional and unambiguous, evidenced by clear affirmative action, and revocable at any time - are set out in Section 6, alongside the Section 5 requirement that Data Fiduciaries give Data Principals clear and plain notice of what personal data will be collected and for what purpose.[16] Chapter III confers on Data Principals the rights to obtain information about their personal data, to correction and erasure, to grievance redressal, and to nominate another person to exercise these rights in the event of death or incapacity. Chapter IV contains "special provisions," including the exemptions discussed in Section 17 below, and Chapter V establishes the Data Protection Board of India ("DPBI") as the principal enforcement body, empowered to investigate complaints, direct remedial action, and impose monetary penalties of up to ₹250 crore per violation.

This architecture represents a significant advance on the IT Act regime: it covers all Data Fiduciaries rather than only body corporates, introduces a general purpose-limitation rule,

[14]Nivedita Saksena and others, 'Rebooting Consent in the Digital Age: A Governance Framework for Health Data Exchange' (2021) 6(Suppl 5) BMJ Global Health e005057.
[15]Digital Personal Data Protection Act 2023, s 7.
[16]Digital Personal Data Protection Act 2023, ss 5–6.

confers a suite of individual rights, and establishes a dedicated enforcement mechanism. Applying generally to the healthcare sector, the Act for the first time brings government hospitals, public health programmes, and the ABDM ecosystem itself within the scope of a statutory data-protection framework, beyond the SPDI Rules' reach as non-"body corporates." The central question, however, is whether a framework designed to span e-commerce, banking, healthcare and every other sector alike is adequate to protect health data - or whether that generality comes at the cost of the sector-specific protection that both the 2019 Bill and the Digital Information Security in Healthcare Act ("DISHA") had separately proposed.[17]

4.2 The Disappearance of "Sensitive Personal Data"

The most significant change between the 2019 Bill and the 2023 Act, for the purposes of this study, is the removal of the tiered classification of personal data. The DPDP Act defines "personal data" simply as any data about an identifiable individual, and imposes a single, uniform set of obligations on all such data regardless of its content or the potential harm arising from its disclosure. There is no equivalent in the 2023 Act to Clause 3(36) of the 2019 Bill,[18] which had defined "sensitive personal data" to include health data, and no category of "health data" attracting specific consent requirements, mandatory data protection impact assessments, or other heightened obligations. Commentary published since the DPDP Rules were notified suggests that, absent a statutory category, guidance on what constitutes health data for compliance purposes must instead be drawn - if at all - from non-statutory instruments such as the Health Data Management Policy and the Electronic Health Record ("EHR") Standards for India, 2016,[19] neither of which derives its authority from the DPDP Act itself.

The Act does contain one mechanism, in principle, for differentiated obligations: the category of "Significant Data Fiduciary" ("SDF"), which the Central Government may designate for a data fiduciary or class of data fiduciaries based on factors including the volume and sensitivity of personal data processed, the risk of harm to Data Principals, and considerations of sovereignty and security. SDFs face additional requirements, including the appointment of a Data Protection Officer based in India, the appointment of an independent data auditor, and periodic data protection impact assessments. As of early 2026, however, the

[17]Centre for Health Equity, Law and Policy, Digital Technology, Health & The Law: Implications for Universal Health Coverage (RTH-UHC Working Paper No 4, 2023).
[18]Personal Data Protection Bill 2019, cl 3(36).
[19]Ministry of Health and Family Welfare, Electronic Health Record Standards for India (n 11).

Central Government had not yet published the criteria or the list of entities to be designated SDFs, so that only the baseline obligations applicable to all Data Fiduciaries currently apply in practice. The SDF mechanism is, in any event, targeted at entities rather than categories of data: it sets no rule for "health data" as such, only for "certain entities" meeting a scale threshold. Not every small entity will meet that threshold, and scale is not necessarily determinative of effective protection in a healthcare system where health data is processed not only by large hospital chains but by a long tail of small clinics, diagnostic centres, telemedicine start-ups and individual practitioners - few of which are likely ever to meet SDF volume thresholds, but which collectively handle data whose sensitivity does not diminish with the size of the entity holding it.[20]

4.3 Section 7: "Certain Legitimate Uses" and Health Data

Section 7 of the DPDP Act[21] lists a range of "certain legitimate uses" that justify processing personal data without the consent otherwise required under Section 6.[22] Several of these bear directly on the use of health information. Section 7(b), which permits the State or its instrumentalities to process personal data for the performance of any function under law, applies straightforwardly to government health schemes such as Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana,[23] which determine eligibility for, and administer, health-insurance benefits on the basis of personal and health-related data. Section 7(f) permits processing without consent where necessary to respond to a medical emergency involving a threat to the life or immediate health of the Data Principal or another individual - for example, allowing an emergency-room physician to access an unconscious patient's medical history through the ABDM without obtaining real-time consent.[24] Section 7(g)[25] permits processing for an epidemic, outbreak of disease, or other threat to public health, enabling a health department to collect and process patient information for contact-tracing or outbreak management. Section 7(h)[26] permits processing for measures taken to ensure individual safety during a disaster or a breakdown of public order, which would extend to health-related data collected in disaster

[20]Centre for Health Equity, Law and Policy (n 17).
[21]Digital Personal Data Protection Act 2023, s 7.
[22]Digital Personal Data Protection Act 2023, s 6.
[23]Udaya Shankar Mishra, Suryakant Yadav and William Joe, 'The Ayushman Bharat Digital Mission of India: An Assessment' (2024) 10(2) Health Systems & Reform 2392290.
[24]ibid.
[25]Digital Personal Data Protection Act 2023, s 7(g).
[26]Digital Personal Data Protection Act 2023, s 7(h).

response. Section 7(i)[27] permits processing of an employee's personal data - including health information obtained in the course of employment - for purposes of employment and to prevent loss or liability to the employer.

Each of these exceptions, considered individually and in the abstract, reflects a defensible policy choice: requiring explicit consent before accessing an unconscious patient's medical records would be impracticable and unsafe, and the collection of health records for public health purposes during an epidemic is a well-accepted restriction on individual privacy. The difficulty lies not in the existence of these exceptions but in the breadth and imprecision of their drafting, the absence of any safeguards attached to their invocation, and the risk that grounds meant for genuinely exceptional circumstances will be invoked more broadly - for instance, for routine health-data analytics, research, or service-improvement purposes unconnected to any emergency.

4.4 Section 17: State and Research Exemptions

Section 17 of the Act[28] provides a further list of exemptions, distinct from the Section 7 "legitimate uses," from Sections 5 to 8 - the notice, consent, purpose-limitation and general obligations that would otherwise apply to Data Fiduciaries. These obligations are waived for processing carried out for research, archiving or statistical purposes, subject to safeguards the Central Government may notify to ensure that a Data Principal's identity cannot be inferred from the resulting data, under Section 17(2)(b). While important for medical research, the protective force of this safeguard depends on standards that, as of the notification of the DPDP Rules in November 2025, remained undefined for health data specifically.

Under Section 17(2)(a), read with Sections 17(4) and 17(5), the Central Government may, by notification, exempt any instrumentality of the State, or class of instrumentality, from the Act on grounds of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or prevention of incitement to a cognisable offence relating to any of these - and may separately grant temporary exemptions of up to five years to any Data Fiduciary or class of Data Fiduciaries, including start-ups. Though framed in general, sector-neutral terms, these exemptions bear particularly on health data, since much of India's health infrastructure - the ABDM, the National Health Authority, State health

[27]Digital Personal Data Protection Act 2023, s 7(i).
[28]Digital Personal Data Protection Act 2023, s 17.

departments, public hospitals, and government health-insurance schemes - qualifies as "instrumentalities of the State" within the meaning of Article 12 of the Constitution[29] and analogous principles of administrative law. The breadth of the grounds for exemption (particularly "public order" and "friendly relations with foreign States"), together with the absence of any requirement of parliamentary approval (as opposed to being merely laid before each House), raises the possibility that significant parts of the public digital health ecosystem could be exempted, by executive notification alone, from the core obligations of notice, consent and purpose limitation - without the judicial or parliamentary review that would ordinarily accompany so substantial a derogation from a statutory privacy regime.

4.5 The DPDP Rules, 2025, and the Implementation Timeline

The DPDP Act remained dormant for more than two years after its enactment, awaiting the rules necessary to make it operational. On 13-14 November 2025, the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025,[30] comprising twenty-two rules and four schedules. The Rules elaborate on the content and form of notices to Data Principals; the registration and operation of "Consent Managers," through which Data Principals can give, review and withdraw consent across multiple Data Fiduciaries; security safeguards for Data Fiduciaries; the timelines and manner of breach reporting; additional safeguards for processing children's data and the data of persons with disabilities; and the constitution and procedure of the Data Protection Board.

Provisions concerning the constitution and functions of the Board, and the Central Government's rule-making and notification powers, came into force on notification in November 2025, while most substantive compliance obligations - including those relating to Consent Managers - become fully effective between November 2026 and May 2027. This staggered timeline has a distinct significance for healthcare: the consent-manager architecture contemplated by the DPDP Rules is structurally similar to, and will likely need to interoperate with, the consent-manager architecture already operating within the ABDM ecosystem. In the interim, health data continues to be processed under the non-statutory consent provisions of the existing Health Data Management Policy. Notably, the DPDP Rules, despite their considerable length, make no reference to health data as a category and do not cross-refer to the Health Data

[29]Constitution of India, art 12.
[30]Digital Personal Data Protection Rules 2025.

Management Policy or the EHR Standards, 2016 - suggesting that the rule-making process was not used as an opportunity to introduce a health-data-specific safeguard of the kind contemplated, for example, by the 2019 Bill's data protection impact assessment provisions.

The "certain legitimate uses" in Section 7 raise distinct proportionality considerations when tested against the constitutional standard in Puttaswamy - that any restriction on the right to privacy be necessary for a legitimate State aim and proportionate to it. Two features of Section 7 warrant particular attention in the health-data context. First, neither the "medical emergency" ground under Section 7(f) nor the "epidemic" ground under Section 7(g) is expressly limited in time or scope to the duration of the emergency or epidemic itself. A Data Fiduciary that lawfully processes a Data Principal's health data during the acute phase of a disease outbreak is not, on the text of the Act, under any express obligation to cease processing once the outbreak subsides, nor to revert to the ordinary consent-based regime. The absence of a sunset clause, post-emergency review, or contemporaneous documentation requirement means there is no statutory mechanism for testing the continuing proportionality of processing once the emergency that justified it has passed; commentators have noted the risk that grounds meant for genuinely extraordinary circumstances could instead be invoked for routine health-data analytics under the broad heading of "public health."

Second, Section 7(b) - permitting the State and its instrumentalities to process personal data for the performance of any function under law, or for the provision of any subsidy, benefit, service, certificate, licence or permit - is drafted broadly enough to capture the entirety of the State's interaction with citizens under health schemes. Combined with the absence of any health-data category under the Act, this subjects the processing of diagnoses, treatment and claims data for tens of crores of Ayushman Bharat-PMJAY beneficiaries to the same general "performance of function" test that would apply to, for instance, the issuance of a driving licence. Under this approach, the proportionality analysis required by Puttaswamy is left almost entirely to the discretion of the executive authority defining the scope of the relevant "function," "benefit" or "service," with no statutory requirement for a health-data-specific impact assessment before such processing is expanded.

5. STATE EXEMPTIONS, SURVEILLANCE AND ACCOUNTABILITY

The exemptions in Section 17(2)(a) and the temporary exemption power in Section 17(5), discussed in Part 4.5, compound the concerns identified above in light of the scale of the

ABDM ecosystem. Because the ABDM and its component registries - the Health ID/ABHA system, the Health Facility Registry, the Health Professional Registry, and the Unified Health Interface - are administered by an instrumentality of the Union Government, an exemption for "instrumentalities of the State" under Section 17(2)(a) could potentially extend to some or all of this infrastructure. The grounds available for such an exemption mirror those historically invoked to justify restrictions on the right to information and on judicial review of executive action in other contexts; applied to a database holding the medical histories of the bulk of the Indian population, they raise a distinct concern about function creep - that a database built for healthcare purposes could, through a security-framed exemption notification, come to be used for non-healthcare purposes, without the knowledge of the Data Principals whose information it contains and without the notice, consent and purpose-limitation protections that would otherwise apply.[31]

These concerns are compounded by the institutional structure of the Data Protection Board of India, which is tasked with enforcing the Act, including against State instrumentalities. Board members are appointed by the Central Government on the recommendation of a selection committee composed largely of senior Central Government officials, and the Board's tenure, terms of service, and removal are likewise governed by rules made by the Central Government.[32] The Act does not address the potential for a conflict of interest between a Board so constituted and a Central Government instrumentality - such as the National Health Authority, or the ministry responsible for a given health scheme - whose processing the Board may be called upon to review. The absence of a more independent appointment mechanism, of the kind proposed under the earlier draft bills (which envisaged a Data Protection Authority with a more varied appointment process), is a structural weakness that bears with particular force on the State's own handling of health information, precisely because Sections 7(b) and 17 already afford the State the most permissive treatment available under the Act.

6. COMPARATIVE PERSPECTIVES

Clause 3(36) of the 2019 Bill had defined "sensitive personal data" to include the "physical, psychological and mental health condition" of an individual, and Clause 27 of the Bill required Significant Data Fiduciaries to conduct a data protection impact assessment

[31]European Data Protection Board, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is Likely to Result in a High Risk (WP248 rev 01, 2017).
[32]Digital Personal Data Protection Rules 2025 (n 30).

before undertaking large-scale processing of sensitive personal data or any processing carrying a risk of significant harm to Data Principals.[33] Both provisions were dropped in the transition from the 2019 Bill to the 2023 Act. The loss of Clause 3(36) means that health data attracts no heightened consent requirement under the DPDP Act; the loss of Clause 27's mandatory-DPIA trigger for sensitive data means that a data protection impact assessment for health-data processing now depends entirely on whether the processing entity happens to be designated a Significant Data Fiduciary - a designation that, as discussed in Part 4.2, remains largely unoperationalised.

The provisions discussed in Parts 4 and 5 above - the medical-emergency exception under Section 7(f), the public-health exception under Section 7(g), and the research exemption under Section 17(2)(b) - would each have operated differently, and with materially different safeguards, had Clause 3(36) been carried forward into the 2023 Act. Its absence, combined with the loss of Clause 27's impact-assessment requirement, leaves the processing of health data exposed to the vulnerabilities identified above: a vague standard for permissible "processing for providing health services," inadequate safeguards against re-identification, expansive grounds for processing without consent, a lack of integration with the ABDM's own consent regime, and the absence of impact assessments prior to large-scale collection.[34]

This Part draws limited comparative reference to two foreign regimes that treat health data, in substantially different ways, as distinct from ordinary personal data: the European Union's General Data Protection Regulation ("GDPR") and the United States' Health Insurance Portability and Accountability Act ("HIPAA").[35] The comparison is not offered to suggest that India ought to adopt either model wholesale - both the GDPR and HIPAA operate within constitutional, administrative and healthcare-financing contexts very different from India's - but to identify the normative function served by each regime's health-data-specific provisions, against which the gaps identified in Part 5 can be assessed.

6.1 The European Union: Special Categories Under the GDPR

The GDPR, like India's 2019 Bill, adopts a categorical approach. Article 9 GDPR[36]

[33]Personal Data Protection Bill 2019, cl 3(36), cl 27.
[34]Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), The EU General Data Protection Regulation (GDPR): A Commentary (Oxford University Press 2020).
[35]ibid.
[36]General Data Protection Regulation (EU) 2016/679, art 9.

prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, or data concerning health, unless one of the exceptions in Article 9(2) applies.[37] These exceptions include the data subject's explicit consent; processing necessary to protect the vital interests of a data subject incapable of giving consent; processing necessary for preventive or occupational medicine, assessment of working capacity, medical diagnosis, or the provision of health or social care; and processing necessary for reasons of substantial public interest in public health, subject to suitable safeguards.

Article 35 GDPR[38] requires a data protection impact assessment for processing likely to result in a high risk to individuals' rights and freedoms, and Article 35(4) specifically identifies large-scale processing of genetic, biometric or health data as an example of high-risk processing warranting such an assessment.[39]

The significance of Article 9 GDPR, for present purposes, lies not in the specific conditions it lists - several of which have rough equivalents in Section 7 of the DPDP Act - but in the default rule from which those conditions operate as exceptions. Where the DPDP Act applies uniformly to all personal data, subject to a set of conditions (consent, specified purposes) and exemptions (Sections 7 and 17), the GDPR establishes a presumption against processing health data, from which the Article 9(2) conditions are exceptions. This distinction has two structural consequences. First, the GDPR places the burden of justification on the controller: processing of special-category data is presumptively unlawful, and the controller must affirmatively establish that one of the Article 9(2) conditions is met, with Article 35's impact-assessment requirement adding a further layer of procedural discipline for large-scale health-data processing. The DPDP Act, by contrast, places the burden on the Data Principal to object: health-data processing is permitted under the Act's general terms unless the Data Fiduciary is a Significant Data Fiduciary that fails to conduct an impact assessment. Second, while the GDPR applies to all personal data, it explicitly identifies certain categories as more sensitive and modifies its baseline requirements accordingly. The DPDP Act recognises no such hierarchy: all personal data not covered by a valid exemption under Sections 7 or 17 is, in effect, treated identically, regardless of its underlying sensitivity. By declining to distinguish

[37]General Data Protection Regulation (EU) 2016/679, art 9(2).
[38]General Data Protection Regulation (EU) 2016/679, art 35.
[39]General Data Protection Regulation (EU) 2016/679, art 35(4).

health data from other personal data, the DPDP Act subjects it to a baseline of protection that is, relative to the GDPR, comparatively weaker.

6.2 The United States: HIPAA's Sectoral Model

The United States lacks a comprehensive federal data-protection law comparable to the GDPR or the DPDP Act, relying instead on a sectoral approach in which specific statutes regulate specific categories of data. Principal among these is HIPAA, which regulates "protected health information" held by "covered entities" (health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically in connection with a HIPAA-covered transaction) and their "business associates" (persons performing functions on a covered entity's behalf that involve access to protected health information).[40]

HIPAA's Privacy Rule applies a "minimum necessary" standard to disclosures of protected health information by covered entities, and its Security Rule mandates administrative, physical and technical safeguards for the storage of protected health information, including a risk-analysis and risk-management requirement and breach-notification obligations calibrated specifically to health information.[41] The HIPAA Privacy Rule further establishes a "safe harbour" de-identification standard, under 45 CFR §164.514(b)(2), under which health data is considered de-identified only where eighteen specified categories of identifier - including name, address, dates, and even city of residence and dates closely tied to an individual's care where these could enable identification - are removed, requiring a fine-grained standard of generalisation before a record qualifies as "de-identified" for HIPAA purposes.[42]

HIPAA's principal limitation, for present purposes, lies in its scope: because it applies only to covered entities and their business associates, a substantial share of health-related data falls entirely outside its reach - fitness trackers, wearable devices, and direct-to-consumer health and wellness apps that do not transmit health information in connection with a HIPAA-covered transaction - reproducing precisely the gap left by the SPDI Rules' "body corporate" limitation.[43] Transplanting HIPAA into Indian law would likely reproduce this gap in a sector-

[40] 45 CFR pts 160, 164 ('HIPAA Privacy Rule' and 'HIPAA Security Rule').
[41] 45 CFR pt 164, subpt C ('HIPAA Security Rule').
[42] 45 CFR §164.514(b)(2).
[43] Akshita Modi, 'Future of Medical Data Privacy with Digital Information Security in Healthcare Act' (2020) 6(1) Journal of Legal Studies and Research 112.

specific rather than a definitional form. HIPAA nonetheless offers, by contrast with the GDPR's categorical approach, a useful model of sector-specific obligations tailored to health data - minimum-necessary disclosure standards, calibrated breach notification, and risk-assessment requirements - of a kind the DPDP Act currently lacks.[44]

6.3 Lessons for India

Neither the GDPR's categorical model nor HIPAA's sectoral model maps neatly onto the framework established by the DPDP Act, but each points to a different method of closing the regulatory gaps identified in Part 5 without extensive amendment of the Act itself.[45] The GDPR comparison suggests that India need not - and, absent the political will to revisit Parliament's removal of Clause 3(36), realistically cannot in the near term - introduce a wholesale categorical distinction; but that India could, by amendment, reintroduce a definition of "sensitive personal data" encompassing health data, attaching three key limitations to its processing: first, a requirement of explicit consent, rather than the DPDP Act's general consent standard; second, a mandatory data protection impact assessment for all large-scale processing of health data, rather than one contingent on the still-unoperationalised Significant Data Fiduciary designation; and third - the most consequential change - a presumption against processing absent one of the Section 7 conditions or a Section 17 exemption, effectively restoring the structure of Clause 3(36) within the 2023 Act.

HIPAA suggests an alternative route through rulemaking, allowing the Central Government to achieve much the same result without legislative amendment. The Central Government could define "health data" for the purpose of future notifications, and specify that such data is subject to explicit consent; it could prescribe health-data-specific safeguards through its rule-making powers under Section 17(2)(b) (notifying safeguards for the research exemption) and under its powers to notify classes of Significant Data Fiduciaries. Such rules could include a health-data-specific de-identification standard; breach-notification timelines calibrated, as under HIPAA, to patient-safety risk; and, most consequentially, a presumption - if not an outright requirement - that healthcare providers above a certain size, and digital health providers integrated with the ABDM architecture, be designated Significant Data Fiduciaries.[46]

[44]ibid.
[45]Christopher Kuner, Lee A Bygrave and Christopher Docksey (n 34).
[46]Udaya Shankar Mishra, Suryakant Yadav and William Joe (n 23).

These two routes are not mutually exclusive, and both inform the concrete recommendations set out in Part 7 below.

7. TOWARDS REFORM: RECOMMENDATIONS

This study proposes the following reforms for consideration by the Central Government and Parliament, directed at closing the gap between the DPDP Act's current framework and the sensitivity of personal health data - while preserving the legitimate public-health purposes that the Act's medical-emergency and public-health exceptions are intended to serve, and without impeding the continued expansion of the ABDM ecosystem.

First, health data should once again be recognised as a distinct category. The DPDP Act should be amended to define "health data" - encompassing, at minimum, physical and mental health records, diagnoses, treatment history, and genetic and biometric data used for health-related authentication - and to attach to its processing a requirement of explicit consent, rather than the Section 6 general consent standard.

Second, large-scale processing of health data should require a data protection impact assessment irrespective of Significant Data Fiduciary status. Before undertaking large-scale processing of health data - including processing carried out under the Section 17(2)(b) research exemption - Data Fiduciaries should be required to conduct a data protection impact assessment, on the model of Article 35 GDPR, rather than have that requirement depend on the as-yet unoperationalised Significant Data Fiduciary designation.[47]

Third, the conditions for processing under Sections 7(f) and 7(g) should be calibrated more precisely to genuine medical emergencies and public health needs. In consultation with healthcare providers, the Central Government should: (i) require, by guidance to Data Fiduciaries, that reliance on Section 7(f) or 7(g) be documented at the time of disclosure, including the nature of the emergency or public health threat relied upon; (ii) establish a presumptive time limit on processing under these provisions, beyond which continued processing would require either informed consent or notification to the Data Principal, absent exigent circumstances; and (iii) require that data collected under these provisions be subject to heightened purpose-specification requirements limiting its subsequent use for unrelated

[47]General Data Protection Regulation (EU) 2016/679, art 35 (n 38).

commercial purposes.

Fourth, the Central Government should notify a health-data-specific de-identification standard under the Section 17(2)(b) research exemption. Personal health data - whether or not otherwise considered de-identified - should not qualify for that exemption absent compliance with conditions ensuring that privacy and security safeguards remain tailored to health data's inherent identifiability. In particular, any safeguards notified under Section 17(2)(b) for health data used in research, archiving or statistical processing should include a precise de-identification standard recognising the ease with which certain demographic details (small or rural districts, rare diagnoses, or precise geographic and temporal information) can render data that would otherwise qualify as de-identified personally identifiable - drawing on the granularity of HIPAA's Safe Harbor standard while adapting it to the Indian demographic and healthcare context.

Fifth, the Board should be empowered to adjudicate DPDP complaints independently of State-instrumentality approval, at least for health-data disclosures. Sections 7(b) and 17, read together, permit the Central Government, State Governments, and hospitals or institutions approved by either to process personal data for any purpose specified in those Sections without recourse to Section 6 or Section 17(1). Because both provisions exempt State-instrumentality processing from the DPDP Act's procedural requirements - including Board review of impact assessments and orders - the Central Government is, in effect, positioned to override any Board decision concerning health-data processing by issuing an approval under these Sections.

Sixth, to preserve the Board's institutional independence in respect of health data, its appointment process should be amended to include at least one member nominated by an independent body, such as the judiciary or civil society, specifically for adjudicating complaints or appeals against Union or State Government instrumentalities that process personal health data.

Seventh, patient-facing rights should recognise the limits of erasure. The DPDP Act should supplement the rights of correction, erasure and grievance redressal under Chapter III with guidance on how a Data Principal's right to seek erasure interacts with statutory medical-record retention requirements, ensuring that patients retain the ability to opt out of secondary commercial uses of their records even where the underlying clinical record cannot itself be deleted.

CONCLUSION

On 11 August 2023, the Government of India did what it had twice declined to do between 2019 and 2022: enact legislation replacing India's patchwork regime of privacy and data-protection law with a comprehensive framework. Three months later, on 13–14 November 2025, that framework was joined by a comprehensive set of implementing rules. India now has a data-protection law. But for healthcare - the sector for which privacy first became a matter of sustained national debate following the 2018 Srikrishna Committee report - the DPDP Act offers a framework that sits uneasily beside the sector-specific safeguards found in both the GDPR and HIPAA. Neither foreign statute is a perfect model. But the GDPR's tiered classification of personal data, and HIPAA's health-specific sensitivity requirements, both recognise, at minimum, that health data differs from other personal data and warrants recognition as such - a recognition India's own federal privacy statute currently withholds.

This is not to suggest that the DPDP Act should or could have replicated the GDPR or HIPAA precisely. This paper has argued, more narrowly, that the Act ought to have recognised health data as a distinct category meriting explicit consent and a mandatory data protection impact assessment regardless of Significant Data Fiduciary status; calibrated the "medical emergency" and "public health" grounds in Section 7 with documentation requirements and temporal limits; and addressed the structural tension between Section 7's consent-free processing grounds and Article 21 of the Constitution with a health-data-specific de-identification standard reflecting health data's distinctive identifiability. These changes would not alter the DPDP Act's basic architecture so much as bring that architecture into closer alignment with both India's constitutional privacy jurisprudence and prevailing international norms. Even implemented piecemeal, through rulemaking where appropriate, they would go a considerable way towards reconciling patient privacy with India's public health objectives. As the ABDM platform continues to integrate every patient's medical history within its digital architecture, the strength of the legal protections attached to that history will be tested in earnest.