International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Health Data Protection: A Comparative Analysis of Telemedicine Data Protection Framework in Global Scenario

Varsha P[1], Dr. Ch. Venkateswarlu[2]

[1]Research Scholar, School of Law, VISTAS, Pallavaram, Chennai-117
[2]Associate Professor, School of Law, VISTAS, Pallavaram, Chennai-117

Abstract
The rapid proliferation of telemedicine services globally has generated unprecedented volumes of digital health data, raising critical questions about the adequacy of existing data protection frameworks. This article undertakes a comparative legal analysis of health data protection regimes governing telemedicine in four jurisdictions: the United States (HIPAA), the European Union (GDPR), the United Kingdom (UK GDPR and Data Protection Act 2018), and Sweden (Patient Data Act). Against this comparative backdrop, the article critically examines India's Digital Personal Data Protection Act 2023 (DPDP Act), arguing that its failure to classify health data as a "special category" requiring enhanced protections constitutes a fundamental regulatory deficit. The analysis reveals that India's approach stands in stark contrast to established international norms, where health data universally receives heightened protection through sector-specific legislation, special category classification, or both. The article further examines the implications of this deficit within India's expanding telemedicine ecosystem, particularly the Ayushman Bharat Digital Mission and the rise of vertically integrated health-tech platforms. The article concludes with specific legislative and policy recommendations, including amendments to the DPDP Act, the establishment of a Health Data Protection Authority, and the development of sector-specific health data governance standards aligned with international best practices.

Keywords: telemedicine, health data protection, DPDP Act 2023, GDPR, HIPAA, special category data, digital health, India

1. Introduction

The global telemedicine market has experienced exponential growth, accelerated dramatically by the COVID-19 pandemic. In India, the government's eSanjeevani platform alone recorded over 150 million teleconsultations by 2024, while private platforms such as Practo, PharmEasy, and MFine collectively serve millions of patients annually (Ministry of Health and Family Welfare [MoHFW], 2024). This digital transformation of healthcare delivery generates vast quantities of sensitive personal health data, including medical histories, diagnostic reports, prescription records, biometric measurements, and mental health assessments. The protection of this data is not merely a technical concern but a fundamental legal imperative rooted in the right to privacy recognized by the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India (2017).

Internationally, the sensitivity of health data has been recognized through its classification as a "special category" of personal data requiring enhanced protections. The European Union's General Data Protection Regulation (GDPR) classifies health data under Article 9 as a special category subject to a general prohibition on processing, with limited exceptions (European Parliament & Council, 2016). The United States, while lacking a comprehensive data protection law, enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, creating a sector-specific regime exclusively for protected health information (PHI) with stringent administrative, physical, and technical safeguards (U.S. Congress, 1996). The United Kingdom, post-Brexit, retained GDPR-equivalent protections through the UK GDPR and the Data Protection Act 2018, supplemented by the Caldicott Principles for health data governance (Department of Health, 1997). Sweden, a pioneer in digital health, governs health data through the Patient Data Act (Patientdatalagen, SFS 2008:355) alongside EU GDPR compliance.

Against this international consensus, India's Digital Personal Data Protection Act 2023 (DPDP Act) represents a conspicuous departure. The Act adopts a principles-based approach to data protection without creating any special category classification for sensitive data types, including health data (Parliament of India, 2023). This article argues that this omission constitutes a critical regulatory deficit that undermines the privacy and security of health data in India's rapidly expanding telemedicine ecosystem. Through a systematic comparative analysis of four jurisdictions, this article identifies the specific protections that India's framework lacks and proposes targeted reforms to bridge this gap.

2. Health Data in the Telemedicine Context: Definitional and Conceptual Framework

Health data in the telemedicine context encompasses a broader range of information than traditional clinical records. The World Health Organization (WHO) defines health data as any data relating to health conditions, the provision of health services, or payment for healthcare (WHO, 2021). In telemedicine, this definition extends to include audio and video recordings of teleconsultations, digital prescriptions, remote patient monitoring data from wearable devices, mental health assessment scores, geolocation data indicating healthcare-seeking behavior, and metadata about consultation patterns and frequencies.

The sensitivity of health data derives from multiple dimensions. First, health data reveals intimate details about an individual's physical and mental condition, creating risks of discrimination in employment, insurance, and social relationships (Gostin & Hodge, 2002). Second, health data is inherently non-fungible — unlike a compromised password, a medical diagnosis cannot be changed or replaced once disclosed (Terry, 2012). Third, in the telemedicine context, health data traverses multiple intermediaries — the patient's device, the internet service provider, the telemedicine platform, cloud storage providers, payment processors, and potentially linked e-pharmacy services — each representing a potential vulnerability point (Kotz et al., 2009). Fourth, the aggregation of health data across platforms enables profiling that may reveal conditions the patient never explicitly disclosed, a phenomenon termed "health data inference" by scholars (Wachter & Mittelstadt, 2019).

The unique characteristics of telemedicine-generated health data necessitate regulatory frameworks that go beyond general data protection principles. As Manson and O'Neill have argued, the traditional notice-and-consent model of data protection is inadequate for healthcare contexts where patients are often in vulnerable positions and cannot meaningfully assess the implications of data processing (Manson & O'Neill, 2007). This recognition has driven the development of sector-specific or special-category protections in jurisdictions with mature data protection regimes.

3. The United States: HIPAA and the Sector-Specific Approach

The United States' approach to health data protection is anchored in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), supplemented by its implementing regulations: the Privacy Rule (45 C.F.R. Parts 160, 164, Subpart E), the Security Rule (45 C.F.R. Parts 160, 164, Subpart C), and the Breach Notification Rule (45 C.F.R. Part 164, Subpart D). HIPAA applies to "covered entities" — health plans, healthcare clearinghouses, and healthcare providers who conduct electronic transactions — and their "business associates" (U.S. Department of Health and Human Services [HHS], 2003).

The HIPAA framework establishes several protections directly relevant to telemedicine. The Privacy Rule creates the category of Protected Health Information (PHI), defined as individually identifiable health information held or transmitted by a covered entity, and establishes a general prohibition on its use or disclosure except for treatment, payment, or healthcare operations, or with patient authorization (HHS, 2003). The "minimum necessary" standard requires covered entities to limit PHI disclosures to the minimum amount needed for the intended purpose. The Security Rule mandates specific administrative safeguards (workforce training, access management, incident response procedures), physical safeguards (facility access controls, workstation security), and technical safeguards (access controls, audit controls, transmission security, encryption) for electronic PHI (HHS, 2013).

For telemedicine specifically, the COVID-19 pandemic prompted the Office for Civil Rights (OCR) to issue enforcement discretion notifications permitting the use of non-HIPAA-compliant communication platforms for telehealth during the public health emergency (HHS Office for Civil Rights, 2020). This temporary relaxation highlighted both the stringency of HIPAA's normal requirements and the tension between regulatory compliance and healthcare access. Post-pandemic, the Federal Trade Commission (FTC) has increased enforcement of health data breaches involving non-HIPAA-covered entities, including telemedicine platforms, under Section 5 of the FTC Act, using the Health Breach Notification Rule (FTC, 2023a).

The strengths of the US approach include its sector-specific focus, detailed technical requirements, substantial penalties (up to $1.5 million per violation category per year), and decades of enforcement experience. However, HIPAA's limitations are well-documented: its coverage gaps exclude health data held by non-covered entities such as health apps and wearable devices; its complaint-driven enforcement model is reactive; and its state preemption framework creates regulatory fragmentation (McGraw & Mandl, 2021). For India, the US model demonstrates that sector-specific health data legislation, despite imperfections, provides substantially stronger protections than general data protection law alone.

3.1. HIPAA Enforcement, HITECH Act, and the FTC's Expanding Role

The enforcement architecture underpinning HIPAA has evolved significantly since its enactment. The HHS Office for Civil Rights (OCR) has resolved over 30,000 complaints and conducted investigations that have resulted in substantial settlements and civil monetary penalties. Among the most notable enforcement actions, Anthem Inc. agreed to a $16 million settlement in 2018 following a data breach affecting nearly 79 million individuals — the largest HIPAA settlement in history (HHS, 2018). In 2019, the University of Rochester Medical Center paid $3 million for failing to encrypt mobile devices containing electronic Protected Health Information (OCR, 2019). Premera Blue Cross settled for $6.85 million in 2020 after a breach compromised 10.4 million records (HHS, 2020). These enforcement actions demonstrate that HIPAA penalties are not merely statutory possibilities but are actively imposed, creating a credible deterrent effect that India's DPDP Act currently lacks.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 substantially strengthened HIPAA's enforcement framework. HITECH introduced tiered penalty structures based on the level of culpability — ranging from $100 per violation for unknowing violations to $50,000 per violation for willful neglect — with annual caps increasing from $25,000 to $1.5 million per violation category (U.S. Congress, 2009). Critically, HITECH extended HIPAA's security and privacy requirements directly to business associates, closing a significant gap in the original statute. HITECH also mandated breach notification requirements for the first time, requiring covered entities to notify affected individuals, HHS, and in cases involving 500 or more individuals, prominent media outlets. The Act further empowered state attorneys general to bring HIPAA enforcement actions, creating a multi-layered enforcement mechanism. Between 2009 and 2024, HITECH-era penalties exceeded $130 million in aggregate settlements (HHS, 2024).

The Federal Trade Commission's role in health data protection has expanded considerably in recent years, particularly concerning entities that fall outside HIPAA's coverage. The FTC's Health Breach Notification Rule, originally promulgated in 2009, was revised in 2023 to clarify its applicability to health apps, wearable device manufacturers, and other non-HIPAA-covered entities that collect health information (FTC, 2023a). The FTC's enforcement actions against GoodRx ($1.5 million penalty for sharing health data with advertising platforms), BetterHelp ($7.8 million for disclosing mental health information to third parties), and Flo Health (consent order for sharing fertility and menstrual data with analytics firms) illustrate the breadth of this jurisdiction (FTC, 2023a; FTC, 2023b). This dual-track enforcement model — HIPAA for covered entities and the FTC Act for non-covered entities — provides a more comprehensive protective net than any single-statute approach. India's framework, which relies entirely on the DPDP Act without any sectoral supplement, has no equivalent mechanism for addressing health data misuse by entities outside the traditional healthcare delivery system.

4. The European Union and United Kingdom: GDPR Article 9 and Special Category Classification

The European Union's General Data Protection Regulation (GDPR), which came into force on 25 May 2018, represents the global gold standard for special category data protection. Article 9(1) of the GDPR establishes a general prohibition on the processing of "special categories of personal data," explicitly including "data concerning health," defined in Article 4(15) as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status" (European Parliament & Council, 2016). This prohibition is subject to ten exhaustive exceptions enumerated in Article 9(2), including explicit consent, employment law obligations, vital interests, substantial public interest, health or social care purposes, and public health.

The GDPR's health data protections operate on multiple levels. At the processing level, Article 9(2)(h) permits health data processing for medical purposes, but only when processed by or under the responsibility of a professional subject to confidentiality obligations. At the technical level, Article 32 requires "appropriate technical and organisational measures" proportionate to the risk, with encryption and pseudonymisation explicitly identified as relevant measures. At the governance level, Article 35 mandates Data Protection Impact Assessments (DPIAs) for processing likely to result in high risk to individuals, with health data processing specifically identified as a trigger. At the enforcement level, violations of Article 9 attract the higher tier of GDPR penalties — up to 20 million euros or 4% of global annual turnover (European Parliament & Council, 2016).

The United Kingdom, following Brexit, retained GDPR-equivalent protections through the UK GDPR (as retained by the European Union (Withdrawal) Act 2018) and the Data Protection Act 2018. The UK framework additionally benefits from the Caldicott Principles, originally articulated in the Caldicott Report of 1997 and subsequently updated, which provide health-sector-specific data governance guidance: justify the purpose, use only when necessary, use the minimum necessary, access on a strict need-to-know basis, understand and comply with the law, and the duty to share can be as important as the duty to protect (Department of Health, 1997; National Data Guardian, 2020). The Caldicott Guardian system, which requires every NHS organisation and local authority to appoint a senior person responsible for health data confidentiality, has no equivalent in any other jurisdiction and represents a unique institutional innovation.

For telemedicine, the UK's Care Quality Commission (CQC) has developed the Digital Technology Assessment Criteria (DTAC), which assesses digital health technologies against clinical safety, data protection, technical security, interoperability, and usability standards before they can be used in NHS services (NHS England, 2021). The Data Security and Protection Toolkit (DSPT) requires all organisations accessing NHS patient data to meet specific data security standards annually. These layered mechanisms — legal (UK GDPR), sector-specific (Caldicott), institutional (CQC/DTAC), and operational (DSPT) — create a comprehensive health data governance architecture that India currently lacks entirely.

4.1. The European Health Data Space and GDPR Enforcement in Health Contexts

The European Commission's proposal for a European Health Data Space (EHDS), introduced in May 2022, represents the next evolutionary step in EU health data governance and carries significant implications for the global regulatory trajectory. The EHDS Regulation, which entered its final trilogue negotiations in 2024, establishes a framework for both primary use (individual healthcare delivery) and secondary use (research, innovation, public health, and policy-making) of electronic health data across the EU (European Commission, 2022). Under the EHDS, patients will have the right to access their health data in a standardised electronic format across any EU member state, and healthcare providers will be required to share patient summaries through a cross-border digital infrastructure called MyHealth@EU. For secondary use, the EHDS creates Health Data Access Bodies in each member state that will process and grant access to anonymised or pseudonymised health datasets under strict conditions, including data minimisation, purpose limitation, and secure processing environments.

The EHDS proposal is significant for India's regulatory discourse for three reasons. First, it demonstrates that even jurisdictions with robust health data protections (GDPR Article 9) continue to strengthen and refine their frameworks rather than treating existing legislation as sufficient. Second, the EHDS explicitly addresses the tension between data protection and health data utility — enabling secondary use for research while maintaining rights-based safeguards — a balance that India's DPDP Act does not attempt. Third, the EHDS creates mandatory interoperability standards for electronic health records, addressing the fragmentation that characterises India's health data ecosystem where platforms like eSanjeevani, ABHA, and private telemedicine services operate on incompatible data standards (European Commission, 2022).

GDPR enforcement actions involving health data further illustrate the practical consequences of special category classification. In 2019, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) imposed a 460,000 euro fine on the Haga Hospital in The Hague after it was found that dozens of employees had improperly accessed a celebrity patient's medical records without adequate

access controls (Autoriteit Persoonsgegevens, 2019). The Portuguese data protection authority (CNPD) fined a hospital in Barreiro 400,000 euros for inadequate access management systems that allowed non-medical staff access to patient records through fake profiles (CNPD, 2018). In 2021, the Finnish data protection authority imposed a 608,000 euro fine on a psychotherapy centre, Vastaamo, which suffered a devastating data breach that led to patient extortion by the hackers — a case that resulted in criminal prosecution and demonstrated the catastrophic real-world consequences of health data breaches (Office of the Data Protection Ombudsman, Finland, 2021). The Swedish Data Protection Authority (IMY) fined Capio St. Goran's Hospital 30 million Swedish kronor (approximately 2.9 million euros) for failing to implement adequate access controls and logging for electronic patient records under both the GDPR and the Patient Data Act (IMY, 2021). These enforcement precedents establish that health data protection obligations are actively supervised and materially penalised — a deterrent architecture entirely absent from India's current regulatory framework.

5. The Swedish Model: Patient Data Act and Integrated Digital Health Governance

Sweden presents a particularly instructive model for telemedicine health data governance due to its combination of EU GDPR compliance, sector-specific legislation, and advanced digital health adoption. The Patient Data Act (Patientdatalagen, SFS 2008:355), enacted before the GDPR, established a comprehensive framework for patient data processing in healthcare that anticipates many of the GDPR's principles. The Act governs the creation, maintenance, and sharing of patient records across all healthcare providers, whether public or private, and establishes patients' rights to access, correct, and restrict processing of their health data (Swedish Parliament, 2008).

Sweden's approach is distinguished by several features relevant to the telemedicine context. First, the Patient Data Act creates a unified legal framework for health data regardless of the technological medium — paper records, electronic health records, and telemedicine-generated data are all subject to the same governance regime. This technology-neutral approach avoids the fragmentation that characterises India's regulation, where different instruments govern different types of health data and digital health technologies. Second, Sweden's national health information exchange infrastructure enables secure data sharing across regional healthcare providers while maintaining patient consent and access controls (Nordgren, 2019). Third, the Health and Social Care Inspectorate (IVO) conducts proactive supervision of health data management, including telemedicine-specific inspections, rather than relying solely on complaint-driven enforcement.

Sweden's experience with private telemedicine platforms provides directly relevant lessons. The rapid growth of digital healthcare companies such as Kry, Min Doktor, and Doktor.se since 2016 generated regulatory challenges similar to those India now faces with platforms like Practo and MFine. The Swedish regulatory response included clarifying that all digital healthcare providers are subject to the same Patient Data Act obligations as physical providers, requiring regional health authority oversight of private telemedicine services, and integrating private telemedicine records into the national health information infrastructure (Anell et al., 2012). India's current framework, by contrast, does not clearly establish whether private telemedicine platforms are subject to the same data governance obligations as hospitals and clinics.

5.1. Sweden's E-Health Infrastructure and Regional Data Governance

Sweden's success in digital health governance is inseparable from its well-developed e-health infrastructure, which provides the technical backbone for implementing the legal protections established

by the Patient Data Act. The 1177 Vardguiden portal, operated by Inera AB (a company owned jointly by Sweden's 21 regions and the Swedish Association of Local Authorities and Regions), serves as the national gateway to digital healthcare services. Through 1177, patients can access medical advice by telephone and online, book appointments, renew prescriptions, view their medical records, and communicate with healthcare providers through secure messaging — all within a unified platform that is subject to the Patient Data Act's governance requirements (Inera, 2023). By 2024, 1177 handled over 35 million logged-in visits annually, making it one of the most widely used public digital health services globally.

The governance of telemedicine data in Sweden operates through a distinctive regional model. Sweden's 21 regions bear primary responsibility for healthcare delivery, including digital health services, and each region functions as a data controller under both the GDPR and the Patient Data Act. This decentralised structure means that health data governance is implemented through regional IT policies and access management frameworks, but within the nationally uniform legal requirements of the Patient Data Act. When a patient uses a private telemedicine platform such as Kry, the platform operates under a contract with the relevant region and is subject to the same data governance obligations as the region's own healthcare facilities. The National Board of Health and Welfare (Socialstyrelsen) sets binding regulations on the content and management of patient records, while the Health and Social Care Inspectorate (IVO) supervises compliance and can impose sanctions for violations (Socialstyrelsen, 2016).

The Swedish model also demonstrates how telemedicine data can be integrated into a broader health information infrastructure without compromising patient privacy. The National Patient Overview (Nationell Patientoversikt, NPO) system enables authorised healthcare providers across regional boundaries to access relevant patient data, but only with the patient's active consent and with comprehensive audit logging that records every access event (Inera, 2023). This consent-and-audit architecture — where data sharing is technically enabled but legally controlled through patient consent and retrospective accountability through audit logs — represents a mature approach to the tension between data interoperability and data protection. India's ABDM aspires to similar interoperability but lacks the statutory data governance framework, the institutional audit capacity, and the decades of implementation experience that underpin Sweden's system.

6. India's DPDP Act 2023: The Absent Special Category

India's Digital Personal Data Protection Act 2023, which received Presidential assent on 11 August 2023, represents the culmination of a legislative journey spanning nearly a decade, from the Justice B.N. Srikrishna Committee Report of 2018 through successive draft bills (Parliament of India, 2023). The Act applies to the processing of digital personal data within India and to processing outside India in connection with offering goods or services to data principals in India. It establishes the rights of data principals (notice, consent, access, correction, erasure, grievance redressal, nomination) and the obligations of data fiduciaries (purpose limitation, data minimisation, accuracy, storage limitation, security safeguards).

The most significant omission in the DPDP Act, from a health data perspective, is the absence of any special category or sensitive personal data classification. The Act's predecessor, the Personal Data Protection Bill 2019, had included "health data" in its definition of sensitive personal data under Clause 3(36), subjecting it to additional processing conditions including explicit consent and purpose limitation (Ministry of Electronics and Information Technology [MeitY], 2019). This provision was removed in the subsequent iterations, and the enacted DPDP Act treats all personal data uniformly, regardless of sensitivity. The Act's Section 4 requires consent for all personal data processing and Section 6 specifies

requirements for valid consent (free, specific, informed, unconditional, unambiguous, with clear affirmative action), but these apply identically to a user's name and to their HIV status or psychiatric diagnosis.

This uniform treatment creates several specific vulnerabilities in the telemedicine context. First, the consent framework does not require explicit or heightened consent for health data processing, unlike GDPR Article 9(2)(a) which requires consent that is "explicit" for special category data — a higher threshold than the standard "unambiguous" consent under Article 6. Second, the Act does not mandate Data Protection Impact Assessments for health data processing, unlike GDPR Article 35(3)(b) which specifically identifies large-scale processing of special category data as triggering a mandatory DPIA. Third, the Act's exemptions under Section 17 — which allow government processing without consent for specified purposes — are not subject to additional safeguards when applied to health data. Fourth, the penalty framework under Section 33, while providing for penalties up to 250 crore rupees, does not differentiate between breaches involving health data and breaches involving less sensitive data categories (Parliament of India, 2023).

The implications of this gap are amplified by the architecture of India's digital health ecosystem. The Ayushman Bharat Digital Mission (ABDM), launched in 2021, aims to create a unified health data infrastructure through the Ayushman Bharat Health Account (ABHA), health information exchanges, and interoperable electronic health records. By 2024, over 550 million ABHA numbers had been generated (National Health Authority [NHA], 2024). The ABDM's Health Data Management Policy (HDMP) attempts to fill the legislative gap through administrative guidelines, establishing consent-based data sharing, purpose limitation, and security requirements (NHA, 2022). However, as administrative policy rather than legislation, the HDMP lacks statutory enforceability, cannot override the DPDP Act's provisions, and is not subject to the penalty framework applicable to statutory violations.

The Supreme Court's landmark decision in Puttaswamy (2017) recognized informational privacy as a facet of the fundamental right to privacy under Article 21 and established the proportionality test for privacy restrictions: legality, legitimate aim, proportionality, and procedural safeguards. The Court specifically identified health data as among the most intimate categories of personal information, with Justice Chandrachud observing that medical records relate to the "most intimate aspects of personal life" (Justice K.S. Puttaswamy v. Union of India, 2017, para 169). The DPDP Act's failure to operationalize this judicial recognition through special category classification arguably falls short of the constitutional mandate articulated in Puttaswamy.

6.1. The Justice Srikrishna Committee Recommendations and What Was Lost

The contrast between the DPDP Act 2023 and its intellectual predecessor — the Justice B.N. Srikrishna Committee Report of 2018, titled 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' — is instructive in understanding what protections were deliberately omitted. The Srikrishna Committee explicitly recommended that certain categories of personal data, including health data, genetic data, biometric data, official identifiers, sexual orientation, caste, religious beliefs, and financial data, be classified as 'sensitive personal data' subject to enhanced processing conditions (Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018). The Committee's rationale was grounded in the recognition that these data categories, if misused, pose heightened risks of discrimination, social exclusion, and psychological harm. For health data specifically, the Committee

noted that disclosure of medical conditions such as HIV/AIDS, mental illness, or reproductive health information could result in severe social stigma in the Indian context.

The Srikrishna Committee recommended several specific protections for sensitive personal data that did not survive into the enacted DPDP Act: (a) processing only on the basis of explicit consent, defined more stringently than ordinary consent; (b) mandatory Data Protection Impact Assessments before initiating processing of sensitive data at scale; (c) restrictions on cross-border transfer of sensitive personal data, requiring that such data be stored on servers located in India (data localisation); (d) a higher standard of purpose limitation, requiring that sensitive data collected for one purpose not be processed for any materially different purpose without fresh consent; and (e) enhanced breach notification obligations, including shorter timelines and mandatory notification to affected individuals (Committee of Experts, 2018). The Personal Data Protection Bill 2019, which was the legislative translation of the Committee's recommendations, incorporated many of these provisions under Clause 3(36) and Chapter III. The subsequent withdrawal of the 2019 Bill and its replacement by the DPDP Act 2023, which excised the entire sensitive data framework, represents a significant regression from the considered recommendations of the expert committee appointed by the Government itself.

6.2. The Pre-DPDP Framework: IT Act 2000, Section 43A, and the SPDI Rules 2011

Prior to the DPDP Act 2023, India's health data protection landscape — while fragmented and inadequate — did contain provisions that offered some recognition of health data sensitivity. Section 43A of the Information Technology Act 2000, inserted by amendment in 2008, imposed liability on body corporates for failure to implement and maintain 'reasonable security practices and procedures' in relation to 'sensitive personal data or information' (SPDI), with compensation payable to affected persons (Parliament of India, 2000). The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, framed under Section 43A, explicitly defined SPDI to include 'medical records and history' alongside other categories such as passwords, financial information, biometric data, and sexual orientation (MeitY, 2011).

The SPDI Rules 2011 imposed several obligations on entities handling sensitive personal data, including health data: obtaining consent before collection, providing a privacy policy, allowing data subjects to review and correct their data, limiting disclosure to third parties without prior permission, and implementing reasonable security practices such as IS/ISO/IEC 27001 certification or government-approved standards (MeitY, 2011). While these rules were widely criticised for their limited enforcement, narrow applicability to 'body corporates,' and absence of a dedicated supervisory authority, they nevertheless represented an acknowledgment that health data warranted differentiated treatment. The DPDP Act 2023, which repeals Section 43A, paradoxically removes this limited recognition without substituting any equivalent differentiated protection. The net effect is that India's health data protection framework has, in certain respects, moved backwards from the position established by the SPDI Rules — a regression that is difficult to justify on any principled basis.

7. Vertical Integration and Platform Risks in Indian Telemedicine

The regulatory deficit acquires additional urgency in the context of India's rapidly consolidating health-tech industry. Unlike the relatively compartmentalised healthcare delivery systems of the US, UK, and Sweden, India's telemedicine ecosystem is characterised by vertically integrated platforms that combine teleconsultation, e-pharmacy, diagnostic services, health records management, and insurance intermediation within a single corporate entity. PharmEasy's acquisition of Medlife and subsequent

integration of teleconsultation, medicine delivery, and diagnostic services exemplifies this trend (Competition Commission of India [CCI], 2024). Practo similarly offers teleconsultation, appointment booking, health records, and insurance services through a unified platform.

Vertical integration creates health data governance challenges that India's current framework is not designed to address. When a patient's teleconsultation data, prescription history, medication purchase records, diagnostic results, and insurance claims are held by a single entity or corporate group, the aggregated data profile reveals significantly more about the patient's health than any individual dataset. The "mosaic theory" of privacy — which recognises that individually innocuous data points can reveal sensitive information when combined — is particularly acute in this context (Solove, 2006). Under HIPAA, different components of such an integrated platform would be subject to distinct regulatory requirements depending on whether they qualify as covered entities or business associates. Under GDPR, the aggregation of health data would trigger DPIA requirements and potentially engage the data minimisation principle. Under India's DPDP Act, no additional obligations arise from data aggregation or vertical integration.

The Competition Commission of India's market study on the digital health sector (CCI, 2020) identified data concentration as a potential competitive concern but did not address the privacy dimensions of this concentration. This institutional gap — with the CCI examining competition implications and the Data Protection Board (once operational) examining data protection compliance, but no body examining the intersection of health data concentration, privacy, and market power — reflects the broader absence of health-data-specific governance in India's regulatory architecture.

7.1. Health-Tech Platform Data Practices and Insurance Sector Implications

An examination of the data practices of India's leading health-tech platforms reveals the practical dimensions of the regulatory deficit. Practo, India's largest digital health platform with over 25 million monthly users, collects consultation records, prescription data, health records uploaded by users, appointment histories, and insurance information through its unified platform (Practo, 2024). Its privacy policy permits data sharing with 'partners' for 'improving services' — language sufficiently vague to encompass a wide range of secondary uses. The platform 1mg (now Tata 1mg following acquisition by Tata Digital), which combines teleconsultation, e-pharmacy, and diagnostic services, collects health data across all three verticals and its privacy policy permits processing for 'analytics,' 'research,' and 'personalisation' purposes (Tata 1mg, 2024). Apollo 24|7, the digital health arm of the Apollo Hospitals Group, integrates teleconsultation with its hospital network, pharmacy chain, and diagnostic centres, creating an unprecedented data aggregation capability spanning both digital and physical healthcare interactions. Tata Health similarly leverages the Tata Group's conglomerate structure to connect health data with broader consumer data ecosystems.

The intersection of telemedicine data with the insurance sector raises particularly acute concerns that India's regulatory framework fails to address. The Insurance Regulatory and Development Authority of India (IRDAI) has progressively encouraged the digitisation of insurance underwriting and claims processes, including the use of electronic health records for risk assessment (IRDAI, 2022). When a patient's telemedicine consultation data — including diagnoses, prescriptions, and even the frequency of consultations — is accessible to insurers, the potential for adverse underwriting decisions based on health data is significant. A patient who seeks a teleconsultation for a mental health concern, for example, may face higher premiums or denial of coverage if that data is shared with or accessible to insurance

underwriters. Under HIPAA, the use of PHI for underwriting purposes is subject to specific restrictions and patient authorization requirements. Under GDPR, such use would constitute processing of special category data for a purpose materially different from the original collection purpose, triggering Article 9 protections and requiring a lawful basis distinct from the original consent. Under India's DPDP Act, no specific restriction prevents the use of telemedicine-derived health data for insurance underwriting, provided that a general consent was obtained at the time of data collection. The IRDAI's data protection guidelines, while requiring insurers to maintain data confidentiality, do not specifically address the acquisition and use of telemedicine-derived health data and lack the statutory force of the DPDP Act (IRDAI, 2022).

8. Comparative Analysis: Mapping the Regulatory Gap

A systematic comparison across the four jurisdictions reveals the extent of India's regulatory divergence from international norms. Along the dimension of data classification, the US classifies health data as Protected Health Information under HIPAA, the EU and UK classify it as special category data under GDPR Article 9, and Sweden subjects it to the Patient Data Act's specific regime. India's DPDP Act provides no differentiated classification. Along the dimension of consent requirements, HIPAA requires individual authorisation for uses beyond treatment, payment, and operations; GDPR requires explicit consent (a higher standard than the baseline "unambiguous" consent); and the Patient Data Act requires informed patient consent with specific disclosure obligations. India's DPDP Act applies the same consent standard to health data as to any other personal data.

Along the dimension of institutional oversight, the US has the HHS Office for Civil Rights with health-data-specific enforcement authority and significant penalties. The UK has the Information Commissioner's Office supplemented by the Caldicott Guardian system and CQC's digital technology assessments. Sweden has the IVO conducting proactive health data inspections. India's Data Protection Board, established under the DPDP Act, has no health-sector-specific mandate, expertise, or inspection framework. Along the dimension of security standards, HIPAA prescribes specific administrative, physical, and technical safeguards for health data. GDPR mandates risk-proportionate measures with special category processing as a risk factor. Sweden's Patient Data Act specifies access controls, logging, and audit requirements. India's DPDP Act requires "reasonable security safeguards" without differentiation by data sensitivity.

Along the dimension of breach response, HIPAA requires breach notification to affected individuals within 60 days, to HHS, and — for breaches affecting 500 or more individuals — to media outlets, with specific risk assessment criteria for determining whether a breach has occurred. GDPR requires notification to the supervisory authority within 72 hours and to data subjects when the breach is likely to result in high risk. India's DPDP Act requires notification to the Data Protection Board and affected data principals, but does not specify timelines or differentiate obligations based on the sensitivity of the breached data.

This comparative mapping demonstrates that India is not merely behind the international curve on one or two dimensions but is systematically deficient across all major parameters of health data protection. The absence of special category classification is not an isolated omission but the foundation of a comprehensive regulatory gap that affects consent, security, oversight, enforcement, and breach response.

8.1. Structured Comparative Framework: Six Dimensions Across Five Jurisdictions

The following structured comparison synthesises the analysis across six key regulatory dimensions for each jurisdiction examined in this article. Dimension 1 — Data Classification: The United States classifies health data as Protected Health Information (PHI) under HIPAA, creating a sector-specific category with defined scope; the European Union classifies health data as special category data under GDPR Article 9, subject to a general processing prohibition; the United Kingdom retains the GDPR Article 9 classification under UK GDPR, reinforced by the Caldicott Principles; Sweden applies dual classification under both GDPR Article 9 and the Patient Data Act (SFS 2008:355); India's DPDP Act 2023 provides no differentiated classification — health data is treated identically to any other personal data.

Dimension 2 — Consent Standard: Under HIPAA, individual authorisation is required for uses beyond treatment, payment, and healthcare operations, with specific content requirements for valid authorisations; under GDPR, explicit consent (Article 9(2)(a)) is required — a standard higher than the baseline 'unambiguous' consent under Article 6; under UK GDPR, the same explicit consent standard applies, supplemented by Caldicott's 'justify the purpose' principle; under the Patient Data Act, informed patient consent with specific disclosure obligations and opt-out rights for the National Patient Overview system applies; under India's DPDP Act, the standard consent requirement (Section 6) applies uniformly to health data and non-sensitive data alike.

Dimension 3 — Security Standards: HIPAA prescribes specific administrative, physical, and technical safeguards through the Security Rule, including mandatory risk analysis, encryption, access controls, and audit logging; GDPR mandates risk-proportionate measures under Article 32, with special category status explicitly elevating the risk assessment; UK GDPR applies identical standards, operationalised through the DSPT and DTAC for health-sector entities; Sweden's Patient Data Act specifies access controls, audit logging of all record access, and role-based authorisation as mandatory requirements; India's DPDP Act requires 'reasonable security safeguards' (Section 8) without differentiation by data type or sensitivity.

Dimension 4 — Institutional Oversight: The US has the HHS Office for Civil Rights with dedicated health data enforcement authority, supplemented by the FTC for non-covered entities and state attorneys general post-HITECH; the EU has national data protection authorities with jurisdiction over GDPR health data provisions, supplemented by the European Data Protection Board for cross-border coordination; the UK has the ICO, supplemented by the Caldicott Guardian system, CQC digital technology assessments, and the National Data Guardian; Sweden has the IMY for GDPR enforcement and IVO for Patient Data Act supervision, conducting proactive health data inspections; India's Data Protection Board under the DPDP Act has no health-sector-specific mandate, expertise, or inspection capacity.

Dimension 5 — Breach Response: HIPAA requires notification to individuals within 60 days, to HHS without unreasonable delay, and to media for breaches affecting 500 or more persons, with a specific four-factor risk assessment; GDPR requires supervisory authority notification within 72 hours and individual notification when high risk is likely; UK GDPR applies the same 72-hour standard; Sweden applies GDPR timelines supplemented by IVO reporting requirements; India's DPDP Act requires notification to the Data Protection Board and affected persons but specifies no fixed timeline and makes no distinction based on data sensitivity. Dimension 6 — Penalties: HIPAA penalties reach $1.5 million per violation category per year, enhanced by HITECH's tiered structure; GDPR penalties reach 20 million

euros or 4 percent of global annual turnover, with Article 9 violations attracting the higher tier; UK GDPR maintains the same maximum penalty structure; Sweden applies GDPR penalty limits supplemented by Patient Data Act sanctions; India's DPDP Act provides for penalties up to 250 crore rupees (approximately 30 million dollars) but does not impose higher penalties for health data breaches.

8.5. Constitutional Imperative: Puttaswamy and the Right to Health Data Privacy

The Supreme Court's nine-judge bench decision in Justice K.S. Puttaswamy v. Union of India (2017) established that the right to privacy is a fundamental right under Articles 14, 19, and 21 of the Constitution. The majority opinion, authored by Justice D.Y. Chandrachud, articulated a four-part proportionality test for evaluating restrictions on the right to privacy: (a) legality — the restriction must be sanctioned by law; (b) legitimate aim — the restriction must serve a legitimate state objective; (c) proportionality — the extent of the restriction must be proportionate to the need; and (d) procedural safeguards — there must be adequate procedural guarantees against abuse (Puttaswamy, 2017, para 180). This test, drawing from the jurisprudence of the European Court of Human Rights and comparative constitutional law, provides the framework against which India's health data protection regime must be evaluated.

Applying the Puttaswamy proportionality test to the telemedicine context reveals significant constitutional deficiencies in the DPDP Act's treatment of health data. On the legality prong, while the DPDP Act provides a legal basis for data processing, it fails to establish a specific legal regime for health data — meaning that the processing of health data by telemedicine platforms operates under the same legal authority as the processing of any non-sensitive data. The absence of health-data-specific legal provisions means that the 'legality' of health data processing rests on generic consent provisions that do not reflect the heightened privacy interests at stake. On the legitimate aim prong, while healthcare delivery is unquestionably a legitimate aim, the DPDP Act does not limit health data processing to healthcare-related purposes; health data collected through telemedicine can be processed for any purpose covered by the broad consent obtained at the point of collection, including commercial analytics, targeted advertising, and insurance underwriting.

On the proportionality prong, the DPDP Act's uniform treatment of all personal data is arguably disproportionate to the constitutional recognition of health data's heightened sensitivity. If the right to privacy is graduated — with more intimate information warranting stronger protection, as Puttaswamy explicitly acknowledges — then a legislative framework that provides identical protection for medical diagnoses and email addresses fails the proportionality requirement. The Court's observation that medical records relate to the 'most intimate aspects of personal life' necessarily implies that the statutory framework must provide commensurate protection. On the procedural safeguards prong, the DPDP Act lacks health-data-specific safeguards: no mandatory Data Protection Impact Assessments for health data processing, no health data-specific breach notification timelines, no requirement for health-sector expertise in the Data Protection Board, and no Caldicott-equivalent guardian system for healthcare organisations.

The constitutional argument is strengthened by reading Puttaswamy alongside the Supreme Court's health rights jurisprudence. In Paschim Banga Khet Mazdoor Samity v. State of West Bengal (1996), the Court held that the right to health is integral to the right to life under Article 21. In Navtej Singh Johar v. Union of India (2018), the Court recognised that the right to privacy encompasses the right to be free from discrimination based on intimate personal characteristics. The convergence of these doctrinal strands — the right to privacy, the right to health, and the right to non-discrimination — creates a compelling

constitutional mandate for health data protection that recognises the unique risks of health data disclosure: discrimination in employment, denial of insurance, social stigma, and the chilling effect on healthcare-seeking behaviour. A telemedicine patient who fears that their mental health consultation data may be shared with employers or insurers may forgo necessary treatment, thereby undermining the very right to health that Article 21 protects. The DPDP Act's failure to establish differentiated health data protections is not merely a policy choice but a potential failure to meet the constitutional standard articulated by the Supreme Court itself.

9. Recommendations for Reform

Based on this comparative analysis, this article proposes four interconnected reforms to address India's health data protection deficit in the telemedicine context.

9.1. Amendment to the DPDP Act 2023

The most direct reform is the introduction of a "special category" or "sensitive personal data" classification within the DPDP Act through amendment. Health data, biometric data, genetic data, data revealing racial or ethnic origin, and data concerning sexual orientation should be classified as sensitive personal data subject to enhanced protections: explicit consent requirements, mandatory Data Protection Impact Assessments, heightened security obligations, restricted automated decision-making, and enhanced breach notification timelines. This approach is consistent with the original intent of the PDP Bill 2019, which included such classification before its removal.

9.2. Sector-Specific Health Data Governance Legislation

Given that the DPDP Act amendment process may be protracted, a complementary approach is the enactment of sector-specific health data governance legislation — an "Indian Health Data Protection Act" modelled on HIPAA's sector-specific approach but incorporating GDPR-standard protections. Such legislation would define the categories of entities subject to health data obligations (healthcare providers, telemedicine platforms, health information exchanges, e-pharmacies, health insurers, health data processors), establish minimum security standards for electronic health data, create health-data-specific consent requirements, mandate interoperability standards, and establish enforcement mechanisms.

9.3. Establishment of a Health Data Protection Authority

Neither the DPDP Act's Data Protection Board nor the National Health Authority currently possesses the combined health-sector expertise and data protection enforcement capacity needed for effective health data governance. A specialised Health Data Protection Authority — either as an independent body or as a specialised division within the Data Protection Board with health-sector expertise — should be established. The UK's Caldicott Guardian model provides a useful template: requiring every healthcare organisation, including telemedicine platforms, to designate a senior official responsible for health data governance would create distributed accountability within the centralised regulatory framework.

9.4. Mandatory Health Data Standards for Telemedicine Platforms

The ABDM's Health Data Management Policy should be elevated from administrative guidelines to legally enforceable standards. Additionally, all telemedicine platforms should be required to undergo health data governance assessment — analogous to the UK's DTAC — before being permitted to operate.

This assessment should cover data minimisation practices, consent management, encryption standards, access controls, audit logging, data retention policies, cross-border data transfer safeguards, and incident response capabilities. Compliance should be a condition for registration under the Clinical Establishments Act 2010 or any future National Telemedicine Act.

10. Conclusion

The global consensus on health data protection is clear: health data is fundamentally different from other categories of personal data and requires enhanced legal protections. This consensus is reflected in the special category classification of the GDPR, the sector-specific regime of HIPAA, the institutional innovations of the Caldicott system, and the integrated governance of Sweden's Patient Data Act. India's DPDP Act 2023, by treating health data identically to all other personal data, stands in stark opposition to this international consensus.

The consequences of this regulatory deficit are not theoretical. India's telemedicine ecosystem processes health data at an unprecedented scale — over 550 million ABHA registrations, 150 million eSanjeevani consultations, and millions of private platform interactions annually. This data traverses vertically integrated platforms that aggregate teleconsultation records, prescription histories, diagnostic results, and insurance claims without any health-data-specific governance obligations. The ABDM's administrative guidelines, while well-intentioned, cannot substitute for legislative protections with statutory enforceability.

The Supreme Court in Puttaswamy recognised health data as among the most intimate categories of personal information and established the constitutional framework for its protection. The DPDP Act's failure to translate this constitutional mandate into statutory protections is not merely a legislative gap but a potential constitutional deficiency. The reforms proposed in this article — DPDP Act amendment, sector-specific legislation, institutional specialisation, and mandatory platform standards — are not aspirational ideals but practical necessities supported by comparative experience and constitutional imperative. India's digital health transformation cannot be built on a data protection framework that fails to recognise the fundamental difference between a patient's medical diagnosis and their shopping preferences.

References

1. Anell, A., Glenngard, A. H., & Merkur, S. (2012). Sweden: Health system review. Health Systems in Transition, 14(5), 1–159.
2. Autoriteit Persoonsgegevens. (2019). Besluit tot het opleggen van een bestuurlijke boete: Haga Hospital. The Hague: AP.
3. CNPD. (2018). Deliberation No. 984/2018: Hospital do Barreiro Montijo. Lisbon: Comissão Nacional de Proteção de Dados.
4. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. New Delhi: Ministry of Electronics and Information Technology.
5. Competition Commission of India. (2020). Market study on e-commerce in India: Key findings and observations. New Delhi: CCI.
6. Department of Health. (1997). Report on the review of patient-identifiable information (Caldicott Report). London: Department of Health.

7. European Commission. (2022). Proposal for a Regulation on the European Health Data Space (COM/2022/197 final). Brussels: European Commission.
8. European Parliament & Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
9. Federal Trade Commission. (2023a). Policy statement on health breach notification rule. Washington, DC: FTC.
10. Federal Trade Commission. (2023b). FTC enforcement action: GoodRx Holdings Inc. consent order (Docket No. C-4798). Washington, DC: FTC.
11. Gostin, L. O., & Hodge, J. G. (2002). Personal privacy and common goods: A framework for balancing under the national health information privacy rule. Minnesota Law Review, 86(6), 1439–1479.
12. IMY. (2021). Decision on administrative fine: Capio St. Göran's Hospital. Stockholm: Integritetsskyddsmyndigheten.
13. Inera. (2023). 1177 Vårdguiden: Annual report on digital health services. Stockholm: Inera AB.
14. Insurance Regulatory and Development Authority of India. (2022). Guidelines on information and cybersecurity for insurers. Hyderabad: IRDAI.
15. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
16. Manson, N. C., & O'Neill, O. (2007). Rethinking informed consent in bioethics. Cambridge University Press.
17. McGraw, D., & Mandl, K. D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. npj Digital Medicine, 4(1), 2.
18. Kotz, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-Care Systems, 1–12.
19. Ministry of Electronics and Information Technology. (2011). Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. New Delhi: Government of India.
20. Ministry of Electronics and Information Technology. (2019). Personal Data Protection Bill, 2019. New Delhi: Government of India.
21. Ministry of Health and Family Welfare. (2024). eSanjeevani: National telemedicine service statistics. New Delhi: MoHFW.
22. National Data Guardian. (2020). Caldicott Principles: A revised set. London: NDG.
23. National Health Authority. (2022). Health Data Management Policy. New Delhi: NHA.
24. National Health Authority. (2024). Ayushman Bharat Digital Mission: Progress report. New Delhi: NHA.
25. Navtej Singh Johar v. Union of India, (2018) 1 SCC 791.
26. NHS England. (2021). Digital Technology Assessment Criteria (DTAC). London: NHS England.
27. Nordgren, L. (2019). The performativity of the service-dominant logic: An empirical study of Swedish digital health services. International Journal of Health Governance, 24(2), 138–150.
28. Office of the Data Protection Ombudsman, Finland. (2021). Decision on Vastaamo data breach. Helsinki: Tietosuojavaltuutetun toimisto.

29. Parliament of India. (2000). Information Technology Act, 2000 (Act No. 21 of 2000). New Delhi: Government of India.
30. Parliament of India. (2023). Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India.
31. Paschim Banga Khet Mazdoor Samity v. State of West Bengal, (1996) 4 SCC 37.
32. Practo. (2024). Privacy policy. Bangalore: Practo Technologies Pvt. Ltd.
33. Socialstyrelsen. (2016). Regulations on the management of patient records (HSLF-FS 2016:40). Stockholm: National Board of Health and Welfare.
34. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564.
35. Swedish Parliament. (2008). Patientdatalagen (Patient Data Act), SFS 2008:355. Stockholm: Riksdag.
36. Tata 1mg. (2024). Privacy policy. Gurugram: Tata 1mg Healthcare Solutions Pvt. Ltd.
37. Terry, N. P. (2012). Protecting patient privacy in the age of big data. UMKC Law Review, 81(2), 385–415.
38. U.S. Congress. (1996). Health Insurance Portability and Accountability Act (Pub. L. No. 104-191). Washington, DC.
39. U.S. Congress. (2009). Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. No. 111-5, Title XIII). Washington, DC.
40. U.S. Department of Health and Human Services. (2003). Standards for privacy of individually identifiable health information: Final rule. Federal Register, 68(34), 8334–8381.
41. U.S. Department of Health and Human Services. (2013). HIPAA Security Rule guidance material. Washington, DC: HHS.
42. U.S. Department of Health and Human Services. (2018). Anthem pays OCR $16 million in record HIPAA settlement. Washington, DC: HHS.
43. U.S. Department of Health and Human Services. (2020). Premera Blue Cross settles HIPAA case for $6.85 million. Washington, DC: HHS.
44. U.S. Department of Health and Human Services. (2024). HIPAA enforcement highlights: Cumulative results. Washington, DC: HHS.
45. U.S. Department of Health and Human Services, Office for Civil Rights. (2019). University of Rochester Medical Center pays $3 million to settle HIPAA violations. Washington, DC: HHS.
46. U.S. Department of Health and Human Services, Office for Civil Rights. (2020). Notification of enforcement discretion for telehealth remote communications during the COVID-19 nationwide public health emergency. Washington, DC: HHS.
47. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494–620.
48. World Health Organization. (2021). Global strategy on digital health 2020–2025. Geneva: WHO.