PATIENT DATA PROTECTION IN INDIA: CONSTITUTIONAL PRIVACY, CONSENT ARCHITECTURE, AND REGULATORY GAPS AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Fidha Farshana, CHRIST (Deemed to be University)

ABSTRACT

The rapid digitisation of India's healthcare ecosystem has fundamentally transformed the relationship between patients, medical institutions, and the State. Initiatives such as the Ayushman Bharat Digital Mission (ABDM), the Ayushman Bharat Health Account (ABHA), [1] telemedicine platforms, and electronic health record infrastructures promise accessibility, interoperability, and efficiency in healthcare delivery. However, these developments simultaneously generate unprecedented volumes of sensitive personal data, the misuse of which can directly affect dignity, autonomy, and equality. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's first comprehensive legislative attempt to regulate personal data governance across sectors, including healthcare. Yet, the Act does not classify health data as a distinct category of sensitive personal data, raising significant constitutional and regulatory concerns. This paper examines whether the DPDP Act provides adequate protection for patient confidentiality within India's emerging digital health ecosystem. It argues that although the statute establishes a foundational framework for consent-based processing [2]and fiduciary accountability, structural gaps persist in consent architecture, emergency processing exceptions, telemedicine compliance, cybersecurity enforcement, and digital literacy barriers that affect meaningful participation in ABDM systems. Drawing on the constitutional right to informational privacy [3]recognised in Justice K. S. Puttaswamy v. Union of India, [4]the paper evaluates the extent to which current health data governance mechanisms satisfy the proportionality standards required under Article 21. It further analyses recent cybersecurity incidents such as the AIIMS ransomware attack [5]as indicators of systemic

[1] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[2] Digital Personal Data Protection Act, 2023, § 6.
[3] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[4] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[5] CERT-In, Advisory on Ransomware Threats to Healthcare Institutions (2022).

vulnerability. [6]

The paper concludes by proposing a regulatory reform roadmap that includes classification of health data as sensitive personal data, strengthening consent infrastructure within ABDM, harmonising telemedicine standards with statutory privacy obligations, and establishing sector-specific health data protection norms consistent with global best practices such as the EU General Data Protection Regulation (GDPR). [7]

Keywords: Patient Data Protection; Digital Personal Data Protection Act, 2023; Informational Privacy under Article 21; Ayushman Bharat Digital Mission (ABDM); Consent Architecture in Digital Healthcare; Telemedicine Regulation in India; Cybersecurity in Health Infrastructure; Health Data Governance in India.

Introduction: Digital Healthcare and the Transformation of Patient Confidentiality

Healthcare delivery in India is undergoing a structural transition from institution-centric documentation systems to interoperable digital health infrastructures capable of integrating patient identity, diagnostic history, prescriptions, insurance coverage, and treatment pathways into unified electronic ecosystems. This transition is largely driven by public digital infrastructure initiatives such as the Ayushman Bharat Digital Mission (ABDM), [8]which seeks to create a federated architecture for seamless exchange of health records across hospitals, laboratories, insurers, and government platforms. At the centre of this architecture lies the Ayushman Bharat Health Account (ABHA), a unique digital identifier designed to enable longitudinal tracking of patient medical histories across providers. [9] While such initiatives significantly enhance administrative efficiency and the accessibility of care, they also raise complex legal questions about ownership, control, storage, processing, and disclosure of health information. Unlike traditional paper-based medical records, digital health data can be replicated, aggregated, profiled algorithmically, and transferred across platforms in real time. The consequences of misuse therefore extend beyond reputational injury to include discrimination in employment, insurance exclusion, targeted surveillance, and erosion of decisional autonomy.

[6] Press Information Bureau, Government of India, Cyber Security Incident at AIIMS New Delhi (Dec. 2022).
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[8] National Health Authority, Government of India, Ayushman Bharat Digital Mission Strategy Overview (2021).
[9] National Health Authority, ABHA Number User Guide (2022).

Historically, patient confidentiality in India evolved primarily through professional ethics rather than statutory guarantees. Medical practitioners were expected to maintain secrecy regarding patient information as part of fiduciary obligations embedded within doctor–patient relationships. However, the emergence of digital health ecosystems has shifted confidentiality concerns from individual practitioners to institutional data governance frameworks involving hospitals, technology platforms, insurers, and the State. As a result, traditional ethical obligations are no longer sufficient to address risks associated with large-scale digital data processing. The enactment of the Digital Personal Data Protection Act, 2023, [10]marks a significant milestone in India's privacy jurisprudence by introducing a comprehensive statutory regime governing the processing of personal data across sectors. The Act establishes obligations for data fiduciaries, creates enforceable consent requirements, prescribes penalties for non-compliance, and recognises individual rights over personal data. Nevertheless, its application within healthcare contexts raises unresolved doctrinal and constitutional questions, particularly because it does not classify health information as a distinct category of sensitive personal data deserving enhanced safeguards.

This omission becomes especially significant in light of the Supreme Court's recognition of informational privacy as an intrinsic component of the right to life and personal liberty under Article 21 [11]of the Constitution. Health data occupies a uniquely intimate position within informational privacy frameworks because it reveals bodily conditions, reproductive choices, psychological histories, genetic predispositions, and lifestyle characteristics that shape both identity and autonomy. The absence of differentiated protection mechanisms for such information risks undermining constitutional guarantees even while statutory compliance appears formally satisfied. Against this background, the present paper examines whether India's current legal framework adequately protects patient data within the emerging digital health ecosystem. It evaluates the consent architecture embedded within the DPDP Act, analyses cybersecurity vulnerabilities exposed by recent institutional breaches, and identifies structural tensions between telemedicine guidelines and statutory privacy obligations. Through constitutional analysis and comparative regulatory insight, the paper argues that meaningful protection of patient confidentiality requires sector-specific safeguards beyond the generalised framework currently provided under the DPDP Act.

[10] Digital Personal Data Protection Act, 2023, § 4.
[11]

Literature Review

The protection of patient data within India's emerging digital healthcare ecosystem has increasingly become a subject of scholarly engagement, particularly following the recognition of informational privacy as a fundamental right under Article 21 of the Constitution. Existing literature on this subject broadly engages with three interconnected areas, namely constitutional privacy jurisprudence, institutional developments within India's digital health infrastructure, and statutory regulation introduced through the Digital Personal Data Protection Act, 2023. Scholarly discussions on informational privacy after *Justice K. S. Puttaswamy v. Union of India* have emphasised that control over personal medical information constitutes an essential component of dignity, bodily autonomy, and decisional freedom. These analyses recognise that health data occupies a uniquely sensitive position within personal data governance frameworks because disclosure may expose individuals to social stigma, employment discrimination, insurance exclusion, and other forms of structural disadvantage. While such scholarship provides a strong constitutional foundation for patient data protection, it often remains focused primarily on doctrinal developments without examining their application within India's rapidly expanding digital healthcare infrastructure. A second body of literature evaluates the institutional transformation of healthcare delivery through initiatives such as the Ayushman Bharat Digital Mission and the Ayushman Bharat Health Account framework. Policy-oriented studies frequently highlight the role of interoperable electronic health record systems in improving accessibility, administrative efficiency, and continuity of care across institutions. At the same time, several commentators have raised concerns regarding the adequacy of consent architecture within these systems, particularly in contexts where participation in digital health platforms is shaped by welfare access considerations and digital literacy disparities. These concerns suggest that procedural consent mechanisms may not always translate into meaningful informational autonomy for vulnerable populations. A third strand of academic writing examines the Digital Personal Data Protection Act, 2023 as India's first comprehensive data governance statute applicable across sectors. While scholars acknowledge that the Act introduces significant improvements in fiduciary accountability, consent-based processing requirements, and enforcement mechanisms, many have also observed that its sector-neutral approach limits the effectiveness of safeguards applicable to highly sensitive categories of personal information such as health data. Comparative analyses frequently emphasise the absence of classification-based protections similar to those available under international frameworks such as the European Union's General Data Protection Regulation.

Recent scholarship addressing cybersecurity vulnerabilities within healthcare infrastructure further strengthens these concerns by demonstrating that large-scale institutional breaches can compromise patient confidentiality and disrupt access to essential medical services. Incidents such as ransomware attacks on major public hospitals have highlighted structural weaknesses within digital health governance systems and underscored the need for sector-specific regulatory safeguards. Despite these important contributions, limited academic work has examined the interaction between constitutional informational privacy, consent architecture within the Ayushman Bharat Digital Mission, telemedicine regulatory standards, cybersecurity enforcement gaps, and statutory protections under the Digital Personal Data Protection Act within a single analytical framework. The present study seeks to address this gap by evaluating the adequacy of patient data protection mechanisms in India's digital healthcare ecosystem and proposing a sector-specific reform framework consistent with constitutional proportionality standards under Article 21.

Research Questions

This paper is guided by the following research questions:Primary Research Question, Whether the Digital Personal Data Protection Act, 2023 provides adequate protection for patient confidentiality within India's emerging digital healthcare ecosystem in light of the constitutional recognition of informational privacy under Article 21.

Secondary Research Questions

1. Whether the absence of classification of health data as a distinct category of sensitive personal data under the Digital Personal Data Protection Act, 2023 weakens safeguards available for protecting patient confidentiality.

2. To what extent the consent architecture within the Ayushman Bharat Digital Mission ensures meaningful informational autonomy for individuals participating in digital health platforms.

3. Whether the consent standards recognised under the Telemedicine Practice Guidelines are consistent with the statutory consent requirements introduced under the Digital Personal Data Protection Act, 2023.

4. Whether existing cybersecurity safeguards applicable to public healthcare institutions

adequately satisfy constitutional proportionality requirements governing protection of informational privacy.

Research Methodology

This study adopts a doctrinal legal research methodology in order to examine the adequacy of patient data protection frameworks within India's evolving digital healthcare ecosystem. The research is primarily based on analysis of constitutional provisions, statutory instruments, judicial decisions, regulatory policies, and institutional frameworks governing digital personal data processing within healthcare systems. The study undertakes a detailed examination of the Digital Personal Data Protection Act, 2023 as the principal statutory framework regulating personal data governance in India, with particular emphasis on its consent architecture, fiduciary obligations, enforcement mechanisms, and exemption provisions applicable to healthcare contexts. The constitutional foundation of patient data protection is analysed through the interpretative framework developed by the Supreme Court in *Justice K. S. Puttaswamy v. Union of India*, particularly the recognition of informational privacy as an essential component of the right to life and personal liberty under Article 21 and the application of the proportionality doctrine to restrictions on privacy rights.

In addition to statutory and constitutional analysis, the study evaluates institutional developments within India's digital healthcare ecosystem, including the Ayushman Bharat Digital Mission, the Ayushman Bharat Health Account framework, and the Telemedicine Practice Guidelines issued by the Government of India. These frameworks are examined in order to assess the effectiveness of consent-based data sharing mechanisms and their compatibility with statutory privacy obligations. The research further incorporates a limited comparative analysis of international data protection standards, particularly the regulatory approach adopted under the European Union's General Data Protection Regulation, in order to identify best practices relevant to classification-based safeguards for health data protection. This comparative perspective is used to evaluate potential reforms capable of strengthening India's existing legal framework. Secondary sources including academic commentaries, policy reports, and publicly available documentation relating to cybersecurity incidents affecting healthcare institutions have also been consulted in order to assess structural vulnerabilities within digital health governance systems. Through this combined doctrinal and comparative approach, the study seeks to evaluate whether existing legal safeguards adequately protect

patient confidentiality within India's expanding digital healthcare infrastructure and to propose recommendations for strengthening sector-specific regulatory protections.

Evolution of Patient Confidentiality in India: From Professional Ethics to Digital Governance

Patient confidentiality has historically been recognised as a foundational principle of medical ethics across legal systems. In India, however, the protection of medical information developed gradually through professional regulation rather than comprehensive statutory intervention. Prior to the emergence of digital healthcare infrastructures, confidentiality obligations primarily operated within the framework of trust-based doctor–patient relationships governed by professional codes issued by regulatory bodies such as the Medical Council of India.

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 imposed a duty upon registered medical practitioners to maintain secrecy regarding patient information except in circumstances involving legal compulsion, public interest considerations, or patient consent. These regulations recognised confidentiality as an essential component of ethical medical practice, yet they did not create enforceable statutory remedies for patients whose information was disclosed without authorisation. Consequently, confidentiality protections remained limited in scope and largely dependent upon disciplinary enforcement mechanisms rather than rights-based legal claims.

The Information Technology Act, 2000 [12]represented one of the earliest legislative efforts to address electronic data protection concerns in India. Section 43A of the Act imposed liability upon body corporates for negligence in implementing reasonable security practices while handling sensitive personal data[13]. Subsequent rules framed under the statute identified medical records and health conditions as forms of sensitive personal data requiring enhanced safeguards. Although these provisions introduced important protections for electronically stored health information, their application remained restricted to corporate entities and did not establish a comprehensive rights-based framework applicable across public health infrastructures. The regulatory landscape underwent further transformation with the

[12] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[13] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

introduction of the Telemedicine Practice Guidelines in 2020[14]. These guidelines legitimised remote consultation mechanisms and recognised telemedicine as an integral component of healthcare delivery in India. Importantly, they introduced the concept of implied consent, in which patients initiate teleconsultations voluntarily. While this provision facilitated rapid expansion of digital healthcare access during the COVID-19 pandemic, it also created ambiguity about the adequacy of consent standards in electronic consultation environments, where patients may not fully understand the implications of creating and storing digital records.

Parallel to these developments, the Government of India initiated the Ayushman Bharat Digital Mission as part of its broader strategy to establish interoperable national health infrastructure. The ABDM introduced a federated architecture enabling the storage and exchange of electronic health records through consent-based access mechanisms managed by digital intermediaries known as consent managers[15]. Unlike centralised databases, the federated model seeks to preserve decentralised control over health records while allowing authorised entities to access information through interoperable interfaces. Although this architecture reflects an attempt to balance efficiency with privacy considerations, its effectiveness depends heavily upon the quality of consent obtained from users and the cybersecurity safeguards implemented across participating institutions. In the absence of strong statutory backing, the Health Data Management Policy governing ABDM operations operates largely as a regulatory guideline rather than enforceable legislation. [16]Consequently, questions remain about the extent to which patients retain meaningful control over their medical information once it is integrated into national digital health networks. The enactment of the Digital Personal Data Protection Act, 2023 therefore represents a critical turning point in the evolution of patient confidentiality in India by introducing enforceable statutory obligations applicable across both public and private sector actors engaged in digital data processing.

The Digital Personal Data Protection Act, 2023: Structure and Application within Healthcare Systems

The Digital Personal Data Protection Act, 2023 establishes India's first comprehensive legislative framework governing the collection, processing, storage, and transfer of digital personal data. The statute is designed to balance individual rights over personal information

[14] Telemedicine Practice Guidelines, Ministry of Health & Family Welfare (Mar. 25, 2020).
[15] National Health Authority, ABDM Consent Manager Framework (2022).
[16] National Health Authority, ABDM Consent Manager Framework (2022).

with the legitimate interests of the State and private sector entities engaged in digital innovation and service delivery. Within healthcare systems, the Act assumes particular significance because hospitals, diagnostic laboratories, telemedicine platforms, insurance providers, and government health missions function as data fiduciaries responsible for processing large volumes of patient information. At the core of the statutory framework lies the concept of consent-based data processing. The Act requires that personal data be processed only for lawful purposes upon obtaining clear and informed consent from the data principal unless specific exemptions apply. Consent must be free, specific, informed, unconditional, and capable of being withdrawn. These requirements are especially important in healthcare contexts where patients often disclose information under conditions of vulnerability and urgency.

The Act further introduces the classification of certain entities as Significant Data Fiduciaries [17]based on factors such as the volume and sensitivity of the data processed, the risk to electoral democracy, the security of the State, and the potential impact on public order. Large hospitals, digital health platforms, and government-operated healthcare databases may fall within this category depending upon the scale of their operations. Significant Data Fiduciaries are required to appoint Data Protection Officers, conduct periodic data protection impact assessments, and implement enhanced compliance mechanisms designed to minimise risks associated with large-scale data processing activities. Another important feature of the Act is its penalty framework, which authorises the imposition of substantial financial penalties for failure to implement reasonable security safeguards or to prevent data breaches. Penalties may extend up to two hundred and fifty crore rupees depending upon the nature and severity of violations. This represents a major shift from earlier regulatory regimes where enforcement mechanisms were comparatively weak and rarely invoked in practice. Despite these advances, the Act adopts a sector-neutral approach to personal data governance rather than recognising healthcare information as a distinct category requiring specialised protection mechanisms. Unlike regulatory frameworks such as the European Union's General Data Protection Regulation, which explicitly classifies health data as sensitive personal data subject to stricter processing conditions, the DPDP Act treats medical information within the same general category as other forms of personal data. This lack of differentiated classification raises concerns about the adequacy of the safeguards applicable to information that directly implicates bodily autonomy and personal dignity. The Act also introduces exemptions permitting the processing of personal

[17]Digital Personal Data Protection Act, 2023, § 10.

data without consent in specific circumstances, including medical emergencies and the provision of health services during epidemics. While such provisions are necessary for ensuring continuity of care in urgent situations, they also create the potential for overbroad interpretation in contexts where emergency processing exceptions may be invoked without adequate oversight mechanisms. Taken together, these features demonstrate that while the DPDP Act establishes an important statutory foundation for data protection within healthcare systems, its effectiveness depends upon the manner in which consent architecture, fiduciary accountability, and exemption provisions are interpreted within rapidly evolving digital health infrastructures.

Constitutional Foundations of Patient Data Protection: Informational Privacy after *Justice K. S. Puttaswamy v. Union of India*

The constitutional legitimacy of patient data protection frameworks in India must be evaluated in light of the Supreme Court's landmark judgment in *Justice K. S. Puttaswamy v. Union of India*, which recognised privacy as a fundamental right [18]protected under Article 21 of the Constitution. The decision marked a transformative moment in Indian constitutional jurisprudence by affirming that informational privacy constitutes an essential component of personal liberty and dignity within a democratic society. The Court emphasised that privacy encompasses an individual's ability to control dissemination of personal information and make autonomous decisions regarding disclosure of intimate details relating to health, family, sexuality, and bodily integrity. In doing so, the judgment established a doctrinal foundation for evaluating statutory frameworks governing digital data processing across sectors including healthcare. Importantly, the Court adopted the proportionality doctrine [19]as the primary standard for assessing constitutionality of State action affecting privacy rights. According to this framework, any restriction upon informational privacy must satisfy four essential requirements: legality, legitimate aim, necessity, and proportionality in the narrow sense. Application of this doctrine within digital health governance contexts requires that statutory frameworks regulating patient data processing be supported by clear legislative authority, pursue legitimate public health objectives, adopt least restrictive means available, and maintain an appropriate balance between individual rights and institutional interests.

Health information occupies a uniquely sensitive position within informational privacy

[18] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[19] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 325. privacy

frameworks because disclosure of such information may expose individuals to social stigma, employment discrimination, insurance exclusion, and psychological harm. Conditions relating to mental health, reproductive health, genetic predispositions, and communicable diseases carry particularly high risks of misuse in contexts where data protection safeguards remain weak or poorly enforced. Consequently, constitutional protection of patient data extends beyond mere confidentiality obligations imposed upon medical practitioners and encompasses broader institutional responsibilities relating to digital governance infrastructures. Within this constitutional framework, the adequacy of the DPDP Act must be evaluated not only in terms of statutory compliance mechanisms but also in relation to its capacity to safeguard dignity-based privacy interests recognised under Article 21. The absence of differentiated safeguards for health data therefore raises important constitutional questions regarding whether existing legislative protections satisfy proportionality requirements applicable to highly sensitive categories of personal information.

The relevance of constitutional privacy protections becomes even more pronounced in contexts involving large-scale digital public health infrastructures such as the Ayushman Bharat Digital Mission, where participation by economically vulnerable populations may be influenced by welfare access considerations rather than fully informed voluntary choice. Ensuring that such systems operate consistently with constitutional privacy guarantees therefore represents a central challenge for contemporary health data governance in India.

Cybersecurity Failures and Institutional Vulnerability: Lessons from the AIIMS Ransomware Attack[20]

The increasing digitisation of healthcare infrastructure has significantly expanded the scale and sensitivity of personal information processed within hospital systems. While digital health platforms promise efficiency and accessibility, they also create attractive targets for cyberattacks that can disrupt critical medical services and expose confidential patient information. One of the most illustrative examples of such systemic vulnerability emerged during the ransomware attack on the **All India Institute of Medical Sciences Delhi** in 2022.

The attack compromised approximately 1. 3 terabytes of patient data, affecting nearly 40 million individuals, [21]and paralysed hospital digital infrastructure for nearly two weeks. During

[20] CERT-In, Advisory on Ransomware Threats to Healthcare Institutions (2022).
[21] Parliamentary Standing Committee on Health & Family Welfare, Cybersecurity Preparedness of Government

this period, medical services reverted to manual record-keeping systems, teleconsultation services were suspended, and administrative operations experienced severe disruption. The incident demonstrated that cybersecurity vulnerabilities within healthcare institutions are not merely technical failures but constitutional concerns affecting access to healthcare, informational autonomy, and institutional trust.

From a legal perspective, the AIIMS breach highlights three structural deficiencies in India's existing health data governance framework. First, the incident highlighted the lack of sector-specific cybersecurity compliance standards for public healthcare institutions. While the Digital Personal Data Protection Act imposes general obligations on data fiduciaries to implement reasonable security safeguards, it does not specify technical benchmarks tailored to high-risk sectors such as healthcare, where the consequences of data compromise extend beyond privacy violations to the disruption of life-saving services. Second, the breach illustrated enforcement asymmetry between public and private actors. Historically, liability frameworks under Indian data protection regimes have been applied more rigorously to private corporate entities than to public hospitals operating under resource constraints and fragmented digital infrastructure systems. The DPDP Act attempts to address this imbalance by imposing obligations across sectors, yet enforcement mechanisms remain institutionally untested within large public health networks.

Third, the attack demonstrated the cascading effects of cyber-incidents within federated digital health ecosystems. Because modern healthcare systems operate through interconnected databases linking hospitals, insurance platforms, and government programmes, vulnerabilities within a single institution can simultaneously compromise multiple layers of digital infrastructure. This interconnectedness raises concerns regarding the resilience of national digital health architecture as a whole. Viewed through the constitutional lens articulated in *Justice K. S. Puttaswamy v. Union of India*, such incidents underscore the State's obligation to ensure that digital governance frameworks incorporating personal data processing satisfy proportionality requirements by implementing adequate safeguards against misuse. Failure to establish sector-specific cybersecurity standards therefore risks undermining the legitimacy of large-scale digital health initiatives designed to expand access to care.

Consent Architecture within the Ayushman Bharat Digital Mission: Structural

Hospitals (2023).

Inequality and Informational Autonomy

A central feature of the Ayushman Bharat Digital Mission is its reliance on consent-based access mechanisms that enable patients to authorise the sharing of their electronic health records across institutions through interoperable digital interfaces. The Ayushman Bharat Health Account serves as the primary identity layer in this architecture by linking individuals to longitudinal medical histories, accessible through consent managers that regulate data exchange requests. In principle, such consent-driven architectures represent an important step toward recognising patient autonomy within digital health governance systems. However, the effectiveness of these mechanisms depends upon whether consent obtained from users satisfies substantive rather than merely procedural standards of voluntariness and informed participation.

One of the most significant challenges affecting consent architecture within ABDM arises from disparities in digital literacy across socio-economic groups. A substantial proportion of individuals enrolled in government-supported health insurance schemes belong to economically vulnerable populations whose participation in digital identity infrastructures is often motivated by welfare access considerations rather than by informed choice about the data-sharing consequences. In such contexts, consent mechanisms risk becoming formalistic compliance tools rather than genuine instruments of informational self-determination. These concerns are reinforced by reports of fraudulent identity generation within ABHA-linked benefit schemes in certain states where intermediaries created duplicate beneficiary identities [22]to claim insurance reimbursements for treatments never received by patients. Such incidents highlight the risk that digital health identifiers may be misused in environments lacking strong verification and monitoring safeguards.

Further concerns have emerged regarding transparency in public dashboards for health insurance platforms operating under the broader Ayushman Bharat framework. Analysts have argued that disclosing patient-level treatment information in publicly accessible dashboards may allow the reconstruction of sensitive medical histories through the triangulation of publicly available data points. Although such disclosures may serve legitimate administrative transparency objectives, they raise questions about compliance with the principles of data minimisation and purpose limitation recognised in global data protection frameworks. Within

[22] Medianama, Privacy Concerns in PM-JAY Dashboard Architecture (2024).

the context of the DPDP Act, these developments raise important questions about whether the consent architecture embedded in ABDM systems satisfies the statutory requirements for consent to be free, specific, informed, and capable of withdrawal. Where participation in digital health infrastructures becomes effectively necessary for accessing public welfare benefits, the voluntariness of consent becomes constitutionally contestable. Ensuring meaningful patient autonomy within national digital health systems therefore requires regulatory mechanisms capable of addressing structural inequalities that limit individuals' capacity to understand and exercise their informational rights.

Telemedicine Practice Guidelines and the Statutory Consent Standard under the DPDP Act

The expansion of telemedicine services during and after the COVID-19 pandemic transformed remote consultation platforms into a permanent feature of healthcare delivery across India. Recognising the importance of such services, the Telemedicine Practice Guidelines issued in 2020 established a regulatory framework that permits registered medical practitioners to provide consultations via digital communication technologies. One of the most distinctive features of the telemedicine regulatory framework is its recognition of implied consent where patients initiate consultations voluntarily through digital platforms. This provision reflects practical considerations aimed at facilitating access to medical advice in situations where obtaining formal written consent may be impractical or unnecessary.

However, the consent standard recognised within the Telemedicine Practice Guidelines appears to conflict with the statutory requirements introduced under the Digital Personal Data Protection Act. The DPDP Act requires consent to be explicit, informed, specific, and unambiguous. In contrast, implied consent operates on the assumption that a patient's initiation of communication constitutes sufficient authorisation for the processing of personal data necessary for providing consultation services. This divergence creates regulatory ambiguity for healthcare providers operating within telemedicine environments. If implied consent satisfies professional guidelines but fails to meet statutory standards applicable to personal data processing, practitioners may face uncertainty regarding compliance obligations when storing consultation records, transmitting prescriptions electronically, or sharing diagnostic information across platforms. From a constitutional perspective, the existence of conflicting consent standards may weaken safeguards protecting informational privacy[23] by permitting

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

processing of sensitive health data without ensuring that patients fully understand the consequences of digital record creation and retention. Harmonisation of telemedicine guidelines with statutory consent requirements therefore represents an important step toward strengthening legal certainty within digital healthcare governance frameworks.

Emergency Processing Exceptions and the Risk of Function Creep

Section 7 of the Digital Personal Data Protection Act permits processing of personal data without consent in specific circumstances including medical emergencies and public-health crises. Such exemptions are essential for ensuring continuity of care during situations where obtaining consent may be impractical or impossible. For example, unconscious patients admitted to emergency wards cannot reasonably be expected to provide explicit authorisation for processing their medical histories prior to receiving treatment.

However, emergency processing provisions must be interpreted carefully to prevent expansion beyond their intended scope. In the absence of clearly defined temporal and functional limits, exceptions permitting non-consensual processing may gradually extend into routine administrative practices justified on broadly defined public-interest grounds. This phenomenon, often described as function creep within data governance scholarship, raises particular concerns within digital health ecosystems where large-scale datasets may be repurposed for secondary uses such as epidemiological modelling, insurance risk assessment, or predictive analytics without meaningful patient oversight. Although such uses may generate valuable public-health insights, they must remain consistent with proportionality requirements governing restrictions upon informational privacy recognised under Article 21. [24]Establishing independent oversight mechanisms capable of reviewing emergency data-processing decisions therefore represents an important safeguard against misuse of statutory exemptions within health-data governance frameworks.

Comparative Perspective: Lessons from the European Union's General Data Protection Regulation

A comparative analysis of international data protection regimes provides valuable insight into regulatory mechanisms that can strengthen safeguards for patient confidentiality in digital healthcare systems. Among such frameworks, the European Union's General Data Protection

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

Regulation represents one of the most influential global models governing processing of personal data across sectors. A defining feature of the GDPR is its explicit classification of health information as a special category of personal data requiring enhanced safeguards. Article 9 of the Regulation prohibits the processing of such data except under narrowly defined circumstances, including explicit consent, public health necessity, or scientific research conducted subject to strong anonymisation standards. By recognising the uniquely sensitive nature of medical information, the GDPR establishes a higher threshold for lawful processing than for ordinary personal data. In addition to classification-based safeguards, the GDPR incorporates principles of purpose limitation, data minimisation, storage limitation, and accountability requiring institutions processing health data to demonstrate necessity and proportionality at every stage of data lifecycle management. Data protection impact assessments are mandatory for high-risk processing activities involving sensitive personal information, thereby ensuring that privacy risks are evaluated prior to implementation of digital health initiatives. Although the DPDP Act introduces several comparable accountability mechanisms, its failure to recognise health data as a distinct category of sensitive personal data limits the effectiveness of these safeguards within healthcare contexts. Adoption of classification-based protections similar to those recognised under the GDPR would therefore represent an important step toward strengthening India's health-data governance framework.

Toward a Sector-Specific Regulatory Framework for Patient Data Protection in India

Ensuring meaningful protection of patient confidentiality within India's digital healthcare ecosystem requires the development of a sector-specific regulatory framework capable of addressing risks associated with large-scale processing of sensitive medical information. While the Digital Personal Data Protection Act establishes an important baseline for personal data governance across sectors, healthcare systems present unique challenges requiring tailored safeguards beyond general statutory provisions. First, legislative recognition of health information as a distinct category of sensitive personal data would align statutory protections with constitutional principles recognising informational privacy as an essential component of personal dignity. Such classification would justify the application of stricter consent requirements, enhanced security standards, and stronger accountability obligations to institutions that process medical records.

Second, harmonising telemedicine regulatory frameworks with the statutory consent standards

introduced under the DPDP Act would eliminate ambiguity for healthcare providers operating in remote consultation environments. Explicit consent protocols integrated into telemedicine platforms would strengthen patient awareness regarding storage and transmission of digital consultation records. Third, establishing mandatory cybersecurity compliance benchmarks for public healthcare institutions would reduce vulnerability to ransomware attacks that can disrupt essential services and compromise patient confidentiality. Adoption of sector-specific audit mechanisms and incident-reporting obligations would further enhance institutional resilience against cyber threats. Fourth, strengthening transparency obligations within the ABDM consent architecture would improve patients' understanding of the secondary uses of health data shared across interoperable platforms. Multilingual consent interfaces and simplified disclosure formats could enhance accessibility for individuals belonging to digitally marginalised populations. [25]Finally, creation of independent oversight mechanisms responsible for reviewing emergency data-processing decisions would ensure that statutory exemptions permitting non-consensual processing remain consistent with proportionality requirements recognised under constitutional privacy jurisprudence.

Conclusion

The transformation of India's healthcare ecosystem through digital governance initiatives is one of the most ambitious public infrastructure projects undertaken in the contemporary welfare state. Platforms such as the Ayushman Bharat Digital Mission promise to improve accessibility, efficiency, and continuity of care by enabling interoperable exchange of patient information across institutions. However, these benefits must be balanced against constitutional obligations requiring protection of informational privacy as an essential component of personal dignity under Article 21. The Digital Personal Data Protection Act, 2023 marks an important step toward establishing a comprehensive statutory framework governing personal data processing across sectors. Yet, its sector-neutral approach limits its effectiveness in healthcare contexts, where medical information occupies a uniquely sensitive position in privacy jurisprudence. Cybersecurity incidents such as the ransomware attack on AIIMS Delhi, structural weaknesses in the ABHA consent architecture, regulatory ambiguity affecting telemedicine platforms, and risks associated with emergency processing exceptions collectively demonstrate the need for stronger, sector-specific safeguards capable of addressing

[25] NITI Aayog, National Strategy for Digital Health (2018).

emerging challenges in digital health ecosystems.

Strengthening patient data protection in India therefore requires a multi-layered regulatory strategy combining constitutional principles, statutory reform, institutional accountability mechanisms, and technological safeguards. Adoption of classification-based protections recognising health data as sensitive personal information, harmonisation of telemedicine consent standards, enhancement of cybersecurity compliance frameworks, and establishment of independent oversight mechanisms would significantly improve the resilience and legitimacy of India's digital healthcare governance architecture. As India continues to expand its digital public infrastructure model across sectors, ensuring meaningful protection of patient confidentiality will remain essential not only for safeguarding individual autonomy but also for sustaining public trust in technology-enabled welfare delivery systems.