 DOI: https://10.5281/zenodo.23310596

Digital Health Infrastructure and Patient Privacy: Is Consent Under the Ayushman Bharat Digital Mission Sufficient to Protect Medical Data?

Manveer Singh Bhagat[1]

© The Author(s), under exclusive licence to Oxford Law Review 2026.

Abstract

India has built one of the world's largest digital health systems in about six years. By mid-2026 the Ayushman Bharat Digital Mission (ABDM) had issued over 93 crore Ayushman Bharat Health Account (ABHA) numbers and linked more than 104 crore health records. Its privacy promise rests largely on a single idea: that patients consent to every flow of their data. This article asks whether consent, as the ABDM operationalises it, is sufficient to protect medical data. Through doctrinal analysis of the constitutional, statutory and policy framework, supported by comparative reference to England and the European Union, it argues that consent is necessary but structurally insufficient. Four weaknesses are identified. Consent is often not fully voluntary at enrolment; it is rarely informed in any meaningful sense; its reach is limited by non-consensual pathways and by the persistence of copies; and it cannot answer harms from security failure, re-identification and misuse. The article concludes that the ABDM needs a statutory footing, enforceable duties on those who hold data, independent oversight and design rules that do not depend on patient vigilance, and it shows how the Digital Personal Data Protection Act 2023 could help supply them.

Keywords: Ayushman Bharat Digital Mission, Medical Ethics, Informed Consent, Medical Law, Health Law, Health Data Privacy

1. Introduction

Consider a hypothetical morning in the outpatient registration queue of a district hospital. A woman in her late fifties, whom we may call Meena, is asked by the clerk for her Aadhaar number and mobile phone. The clerk says it will create a health account that will "save time on the next visit". A one-time password arrives, she reads it out, and the screen shows a fourteen-digit number. She has not been told what an ABHA number is, who can see what is later attached to it, or that she could have declined and still been treated. Somewhere in that exchange she has "consented". (The scenario is illustrative and is not drawn from a documented case.)

The scene is ordinary, which is exactly why it matters. The Ayushman Bharat Digital Mission (ABDM), run by the National Health Authority (NHA), was piloted in 2020 and launched

[1] **National Law Institute University (NLIU), Bhopal, Madhya Pradesh, India;**
✉ **Email: manveerbhagat.bsc@nliu.ac.in**

Copyright © Oxford Law Review. *(editor@oxfordlr.com)*

nationally in September 2021. By mid-2026 the government reported more than 93 crore Ayushman Bharat Health Account (ABHA) numbers and over 104 crore health records linked to them (Press Information Bureau 2026). Few public infrastructures of any kind have scaled so quickly, and none handles information as intimate as a diagnosis, a prescription, a mental health note or a pregnancy.

The ABDM's answer to the privacy question is consent. Records stay with the hospital, laboratory or clinic that created them. They travel only when the patient approves a request through a consent manager, for a stated purpose and a limited time, and the approval can be revoked (National Health Authority 2022; Press Information Bureau 2026). The design has real merit. It avoids a central database of medical histories, and it gives the patient a visible role. Yet "did the patient consent?" is a different question from "is the patient protected?", and much public discussion treats the two as one.

This article examines that gap. Its question is whether consent under the ABDM is sufficient to protect medical data. It argues that it is not, and not mainly because the consent technology is badly built. Consent is being asked to carry weight that no consent mechanism can bear: it must supply voluntariness where patients are dependent, understanding where systems are complex, and security where risks are real. The remedy is to keep consent where it works and to surround it with duties, institutions and design limits that do not depend on the patient's vigilance.

1.1 Scope and Approach

The analysis is doctrinal and policy-oriented. It reads the ABDM's governing documents, principally the Health Data Management Policy (HDMP), alongside the constitutional right to privacy, the Information Technology Act 2000 (IT Act) and the Sensitive Personal Data or Information Rules 2011 (SPDI Rules), and the Digital Personal Data Protection Act 2023 (DPDP Act) with its Rules of 2025. It draws on scholarship on notice and consent and on comparative experience from England and the European Union.

Two limits should be stated. First, the HDMP has been revised, and the version discussed here is the revised draft published for consultation in April 2022; later versions should be checked. Second, the DPDP Act's core obligations are not yet in force. The Rules phase them in, with consent-manager registration from November 2026 and the substantive duties from May 2027 (S.S. Rana & Co. 2025). The article therefore assesses the ABDM as it operates today and as it is about to be reshaped. It does not collect empirical data on patient comprehension, which would strengthen future work.

2. How Consent Works in the ABDM

2.1 The Architecture

The ABDM is best understood as a set of connected building blocks rather than a single database. Individuals receive an ABHA number, a 14-digit identifier that can be created with Aadhaar or a mobile number, together with an address used to log in and receive requests (National Health Authority 2022; Press Information Bureau 2026). Hospitals, laboratories and pharmacies are

Copyright © Oxford Law Review. (editor@oxfordlr.com)

registered as Health Information Providers (HIPs) when they hold records and as Health Information Users (HIUs) when they request them. A Health Information Exchange and Consent Manager (HIE-CM) sits in the middle. It receives requests, puts them to the patient, records the decision and notifies the parties. The records themselves remain with the provider and move between provider and requester only after consent is recorded.

The government describes this federated design as "privacy by design". The Ministry told Parliament in 2022 that the ABDM keeps no centralised repository of health records, that sharing follows the patient's consent, that Health Information Users face purpose-based limits, and that a user may not pass data on without fresh consent (Rajya Sabha 2022). The scale of participation explains why these assurances carry so much weight. By mid-2026, over 5 lakh health facilities and nearly 10 lakh health professionals were on national registries, and 2.72 lakh facilities were using ABDM-enabled software (Press Information Bureau 2026).

2.2 The Consent Artefact

Technically, each approved request produces a consent artefact: a signed, machine-readable record of who may access which records, for what purpose and until when. The patient can see artefacts in a personal health records application and revoke them. Three features of this model matter for what follows. Consent is specific to a request, so there is no standing blanket permission. It is time-limited and revocable. And it attaches to a transfer rather than to the record. Once a user has lawfully received a record, the artefact's expiry or revocation does not by itself recall what has already been copied. In practice, users are expected to honour revocation, but that expectation rests on policy and contract, a point returned to in Part 4.

3. Legal Foundations of Consent and Privacy in Indian Health Care

3.1 Constitutional and Common-Law Foundations

The constitutional starting point is *Justice K.S. Puttaswamy (Retd) v Union of India* (Puttaswamy I 2017), where a nine-judge bench held that privacy is a fundamental right under Article 21 and that it includes informational privacy and control over decisions about one's own body. Medical information sits close to the centre of that protection. The Court also fixed the test for State interference: a restriction must have the backing of law, serve a legitimate aim, be proportionate and come with procedural safeguards. When the Court later upheld the Aadhaar scheme in *Puttaswamy II* (2019), it struck down section 57 of the Aadhaar Act, which had allowed private entities to demand Aadhaar-based authentication. That decision shows judicial wariness of identity use that spreads beyond its statutory purpose, and the concern is relevant here because ABHA numbers can be created with Aadhaar, and the early design leaned on it heavily.

The law of medical confidence and consent adds a second strand. In *Mr 'X' v Hospital 'Z'* (1998; 2003) the Supreme Court accepted that a patient's medical information is held in confidence, but held that the duty is not absolute and may yield where disclosure is needed to protect another person's life or health. In *Samira Kohli v Dr Prabha Manchanda* (2008) the Court said that consent to

Copyright © Oxford Law Review. (editor@oxfordlr.com)

treatment is valid only if the patient has been given adequate information about the nature of the procedure, its risks and the alternatives, and that consent to one procedure does not stretch to another. The point to keep is that Indian medical law has long treated consent as something that follows a conversation. A signature, or a tap on a screen, is not enough on its own.

3.2 Statutory and Policy Framework

Statutory protection has been thin. Section 43A of the IT Act and the SPDI Rules treat medical records and history as sensitive personal data. They require a body corporate to obtain written consent for collection and to state the purpose, to give the provider of information an option to withdraw, and to maintain reasonable security practices (SPDI Rules 2011, rr 3 and 5). But they bind body corporates rather than government institutions, they offer compensation rather than a regulator, and they contain no clear duty to tell a patient about a breach. A bill dedicated to health data, the Digital Information Security in Healthcare Act, was drafted in 2018 and never enacted (Ministry of Health and Family Welfare 2018).

In that vacuum the ABDM relies on its HDMP, first issued in December 2020 and revised in draft in 2022 (National Health Authority 2022; Rajya Sabha 2022). The HDMP borrows the vocabulary of data protection: patients are "data principals", and those who hold or use information are "data fiduciaries". It requires free, informed and specific consent, allows revocation, limits Health Information Users to the purpose for which consent was given and, in the revised draft, adds a duty to notify patients of breaches (MediaNama 2022). But it is a policy instrument. Parliament did not enact it, and it applies to participants in the ecosystem by policy and onboarding rather than by statute.

The DPDP Act is the first general statute. Section 6(1) defines valid consent as free, specific, informed, unconditional and unambiguous, given by a clear affirmative action and limited to the data necessary for the stated purpose. Section 6(4) requires withdrawal to be as easy as giving consent, and section 6(10) places the burden of proving consent on the data fiduciary. Section 7 lists "legitimate uses" that need no consent, including some State benefits and services, medical emergencies and public-health threats. Sections 8 and 33 impose security and breach duties backed by penalties of up to ₹250 crore, and the Rules add detail (Ministry of Electronics and Information Technology 2025). The Act, however, has no special category for health data, and section 17 allows broad exemptions, including for State instrumentalities that the Central Government notifies. Table 1 sets the three regimes side by side.

Feature	ABDM HDMP (revised draft, 2022)	IT Act s 43A and SPDI Rules 2011	DPDP Act 2023 and Rules 2025
Legal status	Executive policy for ecosystem participants	Delegated legislation	Statute; core duties from May 2027

Copyright © Oxford Law Review. (editor@oxfordlr.com)

Feature	ABDM HDMP (revised draft, 2022)	IT Act s 43A and SPDI Rules 2011	DPDP Act 2023 and Rules 2025
Standard of consent	Free, informed, specific; recorded as a consent artefact	Written consent for sensitive data, with stated purpose	Free, specific, informed, unconditional, unambiguous; clear affirmative action (s 6(1))
Withdrawal	Revocation of the artefact	Option to withdraw (r 5(7))	As easy as giving consent (s 6(4))
Processing without consent	Listed situations, criticised as broad	Disclosure to government agencies where legally required (r 6)	Legitimate uses (s 7); exemptions (s 17)
Breach notice	To the ABDM and, in the revised draft, to the patient	No express duty	To the Board and affected persons (s 8(6); Rule 7)
Enforcement	Programme governance and onboarding terms	Compensation (s 43A)	Data Protection Board; penalties up to ₹250 crore
Health data as a category	Core subject of the policy	Sensitive (medical records and history)	No separate category

Table 1. Consent and related safeguards across three regimes

Two features stand out. The most health-specific rules, those in the HDMP, are the least secure in law. The most secure law, the DPDP Act, is the least health-specific. The ABDM sits in the gap, and consent is the one safeguard that all three regimes share.

4. Why Consent Alone Falls Short

A fair objection should be met first. The ABDM's defenders can say that participation is optional, that consent is granular and revocable, and that the architecture was designed to avoid the mistakes of centralised systems. Much of that is true, and nothing here suggests bad faith. The argument is narrower. A well-designed consent layer is a necessary condition of patient protection but not a sufficient one, and the gaps appear in the places where the system most needs to be trusted: at enrolment, at the point of understanding, after a transfer and after a breach.

4.1 Voluntariness at the Point of Enrolment

Free consent assumes a real alternative. In a hospital that assumption is fragile. A patient who is unwell, anxious or waiting in a queue for the third hour is poorly placed to negotiate over a registration form, and the person offering the form usually controls access to care.

Official descriptions present the ABDM as consent-based (Press Information Bureau 2026). The question is how that works at the counter. The government has introduced incentive schemes

Copyright © Oxford Law Review. (editor@oxfordlr.com)

that reward facilities and software providers for adoption and for record linkage (Press Information Bureau 2026). Nothing about that is improper; policymakers want the system used. It does mean that the person asking for a patient's Aadhaar and phone number has reasons of their own to ask. SFLC.in (2022), commenting on the revised HDMP draft, read it as making ABHA issuance a condition of using government facilities and programmes, and argued that this contradicted the claim of voluntariness. MediaNama (2022) reported that the same draft dropped the earlier option for minors to opt out. Whether or not those provisions survive in the current text, they show how easily "voluntary" becomes "expected".

The DPDP Act is alert to the problem, at least on paper. Consent must be unconditional, and a request for more data than the purpose requires is not binding (s 6). Children's data needs verifiable parental consent (s 9). But these rules apply only from 2027, and they will arrive after ABHA numbers have been issued on a scale approaching the whole population.

4.2 Informedness and the Limits of Comprehension

Even when a patient says yes freely, the yes may carry little understanding. The scholarship on notice and consent is unkind to the idea that it should. Solove (2013) calls it "privacy self-management" and argues that people cannot be expected to assess the risks of countless data flows, still less to manage them one at a time. McDonald and Cranor (2008) estimated that reading the privacy policies an average person encounters would take about 200 hours a year. Ben-Shahar and Schneider (2011) showed across many fields that mandated disclosure rarely changes what people understand or do. Acquisti, Brandimarte and Loewenstein (2015) add that privacy choices are shaped by context, framing and defaults, which means that whoever designs the screen shapes much of the answer.

Health makes these problems sharper. The information is intimate, the person deciding may be frightened or in pain, and the consequences of disclosure, such as stigma or the loss of insurance or employment, are remote and hard to picture. In a country where patients use many languages and have very different levels of literacy, a consent request on a small screen from an unfamiliar institution is a demanding thing to evaluate. *Samira Kohli* assumed a clinician who explains. In the ABDM the explanation is largely replaced by a notification. This article has not found a published, independent study of how well patients understand ABDM consent requests, so the argument rests on the general literature and on the design of the system. Such a study would be valuable.

There is a deeper difficulty. Nissenbaum (2010) argues that privacy is about whether information flows fit the norms of the context in which the information was shared. A diagnosis given to a doctor carries norms of care and confidence, and consent offers no assurance that those norms travel with the information. Barocas and Nissenbaum (2014) add that consent cannot cover what is inferred when datasets are combined. A patient can approve a transfer without any grasp of what the recipient might learn from it.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

4.3 Revocation, Copies and Secondary Use

The consent artefact attaches to a transfer. When a patient revokes it, the system records the revocation and notifies the parties, but nothing in the artefact can reach back and retrieve a record already received. The user is expected to honour the revocation and to use the data only for the stated purpose, but that expectation depends on policy, contract and the user's own systems. Who audits compliance, and what a patient can do on learning of a violation, are not obvious from the policy text (National Health Authority 2022). A right to withdraw that cannot easily be checked is worth less than it appears.

Secondary use raises a related issue. Like most health data frameworks, the ABDM's design contemplates uses of anonymised or de-identified data beyond individual care, such as research and planning (National Health Authority 2022). Such uses are sensible and often need no individual consent. But anonymisation is not a guarantee. Rocher, Hendrickx and de Montjoye (2019) estimated that 99.98 per cent of Americans could be correctly re-identified in any dataset using fifteen demographic attributes. Health records carry rich attributes by nature: dates of birth, postcodes, rare diagnoses. If de-identified datasets are released on the strength of a promise that they cannot be traced back, the patient has given no consent and is protected only by a technical claim that may not hold.

4.4 Pathways That Bypass Consent

The ABDM's headline statement is that nothing moves without the patient's consent. The text is more qualified. The revised HDMP draft lists situations in which personal data may be processed without consent. The Internet Freedom Foundation, as reported by MediaNama (2022), objected that one of them was framed so loosely that it could allow significant extraction of data in the name of public health. Some exceptions are plainly right, since nobody wants an unconscious patient's record withheld because no one could tap "approve". The difficulty lies in breadth and discretion.

The DPDP Act follows a similar pattern. Section 7 allows processing without consent to respond to medical emergencies and to provide health services during an epidemic or other public-health threat. It also lets the State process data to deliver benefits and services where the person has previously consented or the data already sits in notified State records (s 7(b), (f), (g)). Section 17(2)(b) exempts research and statistical processing that meets prescribed standards, and section 17(2)(a) exempts State instrumentalities notified by the Central Government on grounds such as security and public order. Section 17(4) relaxes some duties for State processing, including the duty to erase data once its purpose is served (s 8(7)). Large parts of the ABDM are public-sector, so how far consent is the operative safeguard for public-sector flows is a live question. It is more accurate to say that nothing moves without consent except in the circumstances that the policy and the statute list, and that those circumstances will be settled by notifications and rules that patients are unlikely to read.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

4.5 Harms That Consent Cannot Reach

Consent does nothing about security. A patient can give a well-informed and entirely voluntary consent to a hospital that then loses the data. India's recent record is not reassuring. A ransomware attack on the All India Institute of Medical Sciences in Delhi in November 2022 crippled records and hospital services, and in October 2023 a seller allegedly offered personal data of 81.5 crore Indians linked to the Indian Council of Medical Research; the government said there was evidence of leakage but that the data had not been stolen (IANS 2023). Neither incident involved the ABDM, and they should not be read as showing that it is insecure. They show the environment in which it operates.

That environment matters because the federated design cuts both ways. Keeping records with the originating facility avoids a single national store of medical histories, which is a genuine advantage. It also means that security depends on lakhs of endpoints, from large hospitals to single-doctor clinics and laboratories, each with its own resources. The system is only as protected as its weakest connected participant, and nothing in a consent artefact can strengthen that participant. Remedies today are thin: compensation under section 43A of the IT Act, which a patient must pursue and prove, and the HDMP's internal governance. The DPDP Act will add reporting duties and penalties of up to ₹250 crore for failures in security safeguards, but not before May 2027 (DPDP Act 2023, s 8 and Schedule; S.S. Rana & Co. 2025).

Finally, consent cannot reach harms that arise from how data is used rather than from whether it was obtained. Health data is valuable to insurers, employers and marketers. The Ministry has assured Parliament that data is not shared with insurance or pharmaceutical companies without consent (Rajya Sabha 2022). That matters, but the assurance relies on consent doing the protecting, and consent can be made a condition of service. An insurer that requires access to a person's records as the price of cover obtains consent only in a thin sense. As health insurance and government schemes move onto digital rails, such pressures are not hypothetical. Some uses should be off the table whatever the patient says.

5. Comparative Lessons

England's care.data programme is a useful warning. Launched in 2013 to extract general practice records into a national database, it offered an opt-out, but poor public communication left many people unaware of it. The programme was paused in 2014 and closed in 2016. The National Data Guardian's review (2016) concluded that public trust required clearer choices, stronger security standards and honest explanation of how data would be used, and a national data opt-out followed in 2018. The lesson is not that consent failed. It is that legitimacy came from transparency and trusted governance, and that a consent mechanism alone could not restore it.

The European Union shows how a mature regime combines consent with other tools. The General Data Protection Regulation (GDPR) treats health data as a special category (art 9), and explicit consent is only one of several lawful grounds. Article 9(2)(h) allows processing for health care by professionals bound by confidentiality, without a fresh consent each time. The law thus accepts that routine care should not turn on a click, and compensates with professional secrecy,

Copyright © Oxford Law Review. (editor@oxfordlr.com)

purpose limits and an independent supervisory authority. It also recognises the problem of voluntariness: consent is not free where a service is made conditional on unnecessary processing (art 7(4)), and recital 43 notes that consent is unlikely to be free where there is a clear imbalance between the person and the controller, as there often is with public authorities (Regulation (EU) 2016/679). The European Health Data Space Regulation (Regulation (EU) 2025/327) goes further. It gives individuals rights of access and, for secondary use, an opt-out, while placing access under public health data access bodies rather than leaving it to individual choices.

These comparisons should not be pushed too far. India's system is larger, more public-sector and more dependent on assisted digital access than either. But the central point travels. Where health data is concerned, consent is one safeguard among several, and the others, namely duties on those who hold data, limits on use and independent supervision, carry much of the load.

6. Beyond Consent: Building a Protection Framework

6.1 A Statutory Footing

The most important change is to give the ABDM's privacy rules the force of law. At present its key protections rest on a policy that the executive can revise. Two routes are open. Parliament could pass a health-specific statute, reviving the thinking behind the 2018 draft. Or the government could use the DPDP Act to give the ABDM a legal home. Section 10 lets the Central Government designate Significant Data Fiduciaries by reference to the volume and sensitivity of data processed, and designated entities must appoint an India-based data protection officer and an independent auditor and carry out periodic impact assessments. Large hospital networks and the ABDM's own exchange components are strong candidates. Either route should state plainly that health data merits stronger protection than ordinary personal data, a tier the Act does not itself provide.

6.2 Duties That Do Not Depend on Consent

A good test is to ask which protections should survive even if the patient taps "approve" on every request. Four candidates stand out. First, a list of prohibited uses of ABDM-linked data, such as underwriting, pricing, employment screening and advertising, that no consent can unlock. Second, data minimisation and retention limits that apply to every holder. Third, security standards scaled to size, so that a rural clinic is asked for something achievable and a hospital chain for something demanding, with public support for smaller providers. Fourth, a duty to tell patients promptly of a breach, in a language they understand.

These duties reflect the idea of the information fiduciary developed by Balkin (2016) and the case for treating privacy as a matter of trust, set out by Richards and Hartzog (2016). The Srikrishna Committee (2018) had already described the relationship between those who collect data and the people it concerns as fiduciary, and Matthan (2017) argued for moving beyond consent towards accountability. Holders of health data owe duties of care and loyalty because patients depend on them, whatever the patients have clicked. The DPDP Act uses the word "fiduciary" but, arguably, imposes mostly procedural duties. Health deserves more.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

6.3 Independent Oversight and Redress

The NHA both promotes the ABDM and governs its privacy rules. That is understandable at launch, but it is an uncomfortable combination: the body measured on enrolment is also the one that should police shortcomings. An independent route is needed. The Data Protection Board is the obvious forum once the Act is fully in force, though patients will need accessible, multilingual and low-cost ways to reach it.

A related question concerns consent managers. The Rules require registered consent managers to be Indian companies with a minimum net worth, to act on the data principal's behalf and to keep records of consent (Ministry of Electronics and Information Technology 2025; S.S. Rana & Co. 2025). SFLC.in (2022) asked whether private entities may serve as consent managers within the ABDM, and the DPDP framework makes that question more pressing. Whether the ABDM's own HIE-CM will need to register, whether independent managers will be allowed to operate alongside it, and how the two models fit together are open. A consent manager answerable to the patient has real value. One answerable to the programme that depends on enrolment has less.

6.4 Better Consent, Used Where It Belongs

None of this means abandoning consent. Consent still has the strongest claim where a use is optional, unusual or commercial, such as sharing records with a new provider for a second opinion, joining a research study or giving an insurer access. For those flows the design should be better than it is. ABHA creation should be separated from treatment and registration, should never be a condition of being seen, and should be offered by someone able to explain it. Requests should be in plain language, in the patient's own language, and say in a sentence who is asking, why and for how long. Defaults should be the shortest duration and narrowest scope. Patients should be able to see an access log showing who has looked at their records, and to revoke everything at once. Assisted consent, through a trusted health worker or family member with clear safeguards, would help patients who struggle with smartphones. This echoes *Samira Kohli*: consent in medicine works when a human being makes sure the patient understands.

7. Conclusion

Meena, the patient in the opening scene, did consent in the narrow sense that matters to the system. A code was entered and a record was created. Whether she was protected is a different question, and this article has argued that the answer depends on much more than that code.

The ABDM's consent architecture deserves credit. It is federated rather than centralised, purpose-limited, time-bound and revocable, and it gives patients a visible role. The question was whether that is sufficient. It is not, for four reasons. Enrolment pressures can hollow out voluntariness. Informed consent is hard to achieve in a hurried, multilingual and digitally unequal setting. Consent attaches to transfers rather than copies, and it coexists with exceptions and with

Copyright © Oxford Law Review. (editor@oxfordlr.com)

de-identified uses that rely on technical promises. And consent has nothing to say about breaches, weak endpoints or uses that patients would never knowingly accept.

The remedy is to put consent in its proper place. It should remain central for optional and commercial flows, and it should be improved. But the base layer of protection should rest on law: a statutory footing for the ABDM, a health-sensitive tier within the DPDP framework, duties of care and loyalty on every holder of data, prohibitions that consent cannot override, breach notification to patients, and oversight by a body that does not also promote enrolment. The phased commencement of the DPDP Rules, from consent-manager registration in November 2026 to the substantive duties in May 2027, offers a window to do this. A system that now touches most of the country should not be left to depend on a one-time password read out at a registration desk.

References

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015) 'Privacy and Human Behavior in the Age of Information', Science, 347(6221), 509–514.

Balkin, J.M. (2016) 'Information Fiduciaries and the First Amendment', UC Davis Law Review, 49(4), 1183–1234.

Barocas, S. and Nissenbaum, H. (2014) 'Big Data's End Run around Anonymity and Consent', in Lane, J. et al. (eds), Privacy, Big Data, and the Public Good. Cambridge: Cambridge University Press, 44–75.

Ben-Shahar, O. and Schneider, C.E. (2011) 'The Failure of Mandated Disclosure', University of Pennsylvania Law Review, 159(3), 647–749.

Digital Personal Data Protection Act 2023 (Act No. 22 of 2023) (India).

Digital Personal Data Protection Rules 2025 (Ministry of Electronics and Information Technology, G.S.R. 846(E), 13 November 2025) (India).

European Parliament and Council (2016) Regulation (EU) 2016/679 (General Data Protection Regulation).

European Parliament and Council (2025) Regulation (EU) 2025/327 on the European Health Data Space.

IANS (2023) 'From AIIMS Delhi to ICMR, data breaches haunt crores of Indians', 12 November. Available at: https://greaterkashmir.com/world/from-aiims-delhi-to-icmr-data-breaches-haunt-crores-of-indians

Information Technology Act 2000 (India), s 43A.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (G.S.R. 313(E)) (India).

Copyright © Oxford Law Review. (editor@oxfordlr.com)

Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (Puttaswamy I).

Justice K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (Puttaswamy II).

Matthan, R. (2017) Beyond Consent: A New Paradigm for Data Protection, Takshashila Discussion Document 2017-03. Bengaluru: Takshashila Institution.

McDonald, A.M. and Cranor, L.F. (2008) 'The Cost of Reading Privacy Policies', I/S: A Journal of Law and Policy for the Information Society, 4(3), 543–568.

MediaNama (2022) Report on the revised Health Data Management Policy, June. Available at: https://www.medianama.com/2022/06/223-new-health-data-management-policy/

Ministry of Health and Family Welfare (2018) Digital Information Security in Healthcare Act (DISHA) (draft). New Delhi: Government of India.

Mr 'X' v Hospital 'Z' (1998) 8 SCC 296; Mr 'X' v Hospital 'Z' (2003) 1 SCC 500.

National Data Guardian (2016) Review of Data Security, Consent and Opt-Outs. London: National Data Guardian.

National Health Authority (2022) Health Data Management Policy, Draft Version 2, April. New Delhi: Government of India.

Nissenbaum, H. (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

Press Information Bureau (2026) Ayushman Bharat Digital Mission, Ministry of Health and Family Welfare, 6 July. Available at: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2026/jul/doc202676912801.pdf

Rajya Sabha (2022) Health Data of Patients, Question No. 258, answered 20 December. Ministry of Health and Family Welfare. Available at: https://rsdebate.nic.in/bitstream/123456789/734275/1/PQ_258_20122022_S140_p39_p45.pdf

Richards, N. and Hartzog, W. (2016) 'Taking Trust Seriously in Privacy Law', Stanford Technology Law Review, 19, 431–472.

Rocher, L., Hendrickx, J.M. and de Montjoye, Y.-A. (2019) 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models', Nature Communications, 10, 3069.

S.S. Rana & Co. (2025) 'MeitY Notifies Final Digital Personal Data Protection Rules 2025'. Available at: https://ssrana.in/articles/meity-notifies-final-digital-personal-data-protection-rules-2025/

Samira Kohli v Dr Prabha Manchanda (2008) 2 SCC 1.

Copyright © Oxford Law Review. (editor@oxfordlr.com)

SFLC.in (2022) Comments on the Draft Health Data Management Policy, Version 02. Available at: https://sflc.in/sflcins-comments-draft-health-data-management-policy-version-02

Solove, D.J. (2013) 'Privacy Self-Management and the Consent Dilemma', Harvard Law Review, 126(7), 1880–1903.

Srikrishna Committee (2018) A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. New Delhi: Ministry of Electronics and Information Technology.

Publisher's Note

Oxford Law Review remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. Oxford Law Review or its licensors retain the rights to this article pursuant to the applicable publishing agreement with the author(s) or other rightsholder(s). Any self-archiving, reproduction, distribution, or reuse of the accepted manuscript or published version is subject to the terms of the applicable publishing agreement and applicable law.

Copyright © Oxford Law Review. *(editor@oxfordlr.com)*