*Page 3734 - 3749* **DOI:** *https://doi.org/10.63108/IJLMH.13096*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

**Volume 9 | Issue 5**

**2026**

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

# Digital Health Surveillance in Public Health Emergencies: Testing the DPDP Act, 2023 Against India's COVID-19 Experience

EKSHITA GOEL*

**ABSTRACT**

*The COVID-19 pandemic accelerated the adoption of digital health surveillance across India, prompting government bodies to deploy contact tracing applications, location tracking and geo-fencing to manage public health risks. These rapid technological interventions, however, raised serious constitutional and data privacy concerns, particularly about the handling of sensitive health information without robust statutory backing. This paper evaluates India's pandemic-era digital health measures through the constitutional lens of* K.S. Puttaswamy v. Union of India *(2017) and assesses the evolution of the governing legal framework. It shows how the legacy framework under the Information Technology Act, 2000 and the IT Rules, 2011 proved structurally incapable of regulating State-led health surveillance. The paper then examines the Digital Personal Data Protection (DPDP) Act, 2023 and the DPDP Rules, 2025, scrutinising in particular the broad 'legitimate use' exceptions for public health emergencies, the State exemptions, data principal rights and executive oversight of the Data Protection Board. It argues that while the DPDP Act provides a long-awaited statutory base, significant regulatory gaps remain. To ensure that public health interventions respect fundamental rights, the paper proposes statutory safeguards, binding emergency protocols and enhanced judicial and institutional oversight.*

***Keywords:*** *Privacy, Personal data protection, COVID-19 pandemic, Digital technology, Health, Digital Personal Data Protection Act 2023, Public health emergency*

## I. INTRODUCTION

Public health emergencies demand swift access to actionable data to trace infection vectors, allocate medical resources and monitor high-risk zones. It has been nearly half a decade since the global spread of COVID-19, but digital health records remain of the first importance in an increasingly interconnected and digitised world. Because future public health emergencies are a recurring possibility rather than isolated events, safeguarding privacy robustly within these digital frameworks is imperative.

* Author is a Ph.D. Research Scholar at National Law University Delhi, New Delhi, India. ORCID: https://orcid.org/0009-0006-5996-8878

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

During the COVID-19 crisis, Indian authorities relied heavily on digital surveillance tools that used personally identifiable data such as cellular location logs, contact graphs, biometric checks and health status. Dar and Wani record that digital technologies were used for tracing, monitoring, testing, vaccine registration and patient databases, all of which hold personally identifiable information such as addresses, phone numbers, identity document numbers and vaccination status.[1] As the OECD has observed, in any public health crisis an effective frontline response requires information on the virus's spread: where it is spreading, how many new cases have been confirmed, how many people have recovered or died, and where it first emerged. Data is also needed to assess containment and mitigation measures, which may limit people's mobility. Geo-location data, acquired through call data records or mobile applications, and biometric data, chiefly facial recognition data,[2] are two types of information on which governments rely for frontline responses. Mapping an epidemic with such data improves the speed, accuracy and efficacy of the medical and administrative response. While digital interventions can improve administrative efficiency during epidemics, large-scale collection of personal data by State and private entities creates acute risks to individual privacy.

Governments must therefore be cautious about the privacy and data protection consequences of using digital technology to combat a public health crisis. As Matthan observes, one class of these technologies drew on the vast stores of personal information held by telecom and social media companies; all of them gathered what he calls "deeply personal data that no-one (private company or government entity) would have had any justification collecting had it not been for the extreme situation"; and where the State coerced their use, the legitimacy of its action was open to question even in exceptional times.[3] The constitutional validity of State surveillance rests on the three-fold test laid down by the Supreme Court in *K.S. Puttaswamy (Retd.) v. Union of India*:[4] legality, necessity and proportionality. Under this standard, any State infringement of informational privacy must be backed by law, pursue a legitimate aim and be proportionate to that aim.

In the absence of a dedicated data protection statute during the height of the pandemic, the collection and processing of health data were governed primarily by the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices

[1] Mohamad Ayub Dar & Shahnawaz Ahmad Wani, *COVID-19, Personal Data Protection and Privacy in India*, 15 ASIAN BIOETHICS REV. 125 (2023), https://doi.org/10.1007/s41649-022-00227-0.
[2] ORG. FOR ECON. CO-OPERATION & DEV., *Ensuring Data Privacy as We Battle COVID-19* (Apr. 14, 2020), https://doi.org/10.1787/36c2f31e-en; Rahul Matthan, *The Privacy Implications of Using Data Technologies in a Pandemic*, 100 J. INDIAN INST. SCI. 611 (2020), https://doi.org/10.1007/s41745-020-00198-x.
[3] Matthan, *supra* note 2, at 611–12.
[4] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the 2011 Rules), instruments designed for commercial data handling rather than State-led epidemiological tracking.

Technological advances undoubtedly improve our lives, but it is equally important that users' right to privacy be respected in major data collection initiatives. For the public to feel comfortable sharing their information, they need a secure and reliable environment in which they can be assured of its safekeeping. A comprehensive regulatory framework for data protection is therefore essential to address user privacy, accountability and data security, and to require the government to comply with specific legal requirements when it acquires people's personal information. Given the need to strike a fair balance between individual rights and the public interest, the technological interventions employed during COVID-19 call for close analysis.

This paper analyses India's digital public health responses to determine whether future health crises can be managed in a privacy-compliant manner. Part II reviews the privacy vulnerabilities exposed by pandemic-era surveillance applications. Part III contrasts the legacy IT Act framework with the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 (DPDP Rules), and evaluates whether the new regime satisfies the constitutional mandate of *Puttaswamy*. Part IV offers policy suggestions to balance public health imperatives with informational privacy.

## II. USE OF TECHNOLOGY IN COVID-19 AND DATA PRIVACY CONCERNS

To curb the transmission of COVID-19, State and Central authorities in India deployed a range of digital surveillance mechanisms. These tools fell broadly into two functional categories: contact tracing systems and home-quarantine monitoring tools.

### A. Digital contact tracing and voluntary consent frameworks

Contact tracing, as Matthan explains, is designed to record everyone with whom a person has come into contact, so that when that person tests positive for COVID-19 those contacts over the preceding days can be identified and given priority testing, allowing them to isolate before they, too, spread the disease, even if they show no symptoms.[5]

The Central Government's primary digital intervention was the Aarogya Setu application, which used Bluetooth proximity sensing and GPS location data and collected each user's name, phone number, age, sex, profession, smoking history and countries visited in the previous 30 days to

[5] Matthan, *supra* note 2, at 613.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

build contact graphs and alert users to potential exposure.[6] Similar applications, such as the Indian Institute of Science's GoCoronaGo, operated on a comparable technical architecture.[7] These applications relied on the Bluetooth capability of mobile phones to detect proximity and build contact networks for automated risk alerts. When two devices running such an application came within close range, they exchanged identifying details of the users, together with location data and the duration and proximity of the contact. If a user later tested positive for COVID-19, Aarogya Setu uploaded the contact information stored on that user's device to a Government server, where it was analysed to identify, alert and arrange medical attention for the contacts at risk.[8] To protect user privacy, the contact data held on the device was encrypted and could not be read even by the user, which protected the identities of his or her contacts, and records not uploaded were deleted from the device on a rolling 30-day cycle.[9]

From a legal perspective, Aarogya Setu presented serious constitutional difficulties. The application was launched through executive directives and accompanied by a data-sharing protocol issued under the Disaster Management Act, 2005, rather than by legislation enacted by Parliament for the purpose.[10] Although the Government presented the app as voluntary, it briefly required employees to use the app during the early lockdowns, and Matthan notes the concern this raised about whether consent given under the app's privacy policy was truly free.[11] The app's privacy policy also contained broad data-sharing clauses, permitting personal information to be shared with "such other necessary and relevant persons" in order "to carry out necessary medical and administrative interventions".[12] Critics faulted the Government for not releasing the source code for independent review and for not demonstrating that the data had been properly anonymised.[13] Further, the policy stipulated that data stored on government servers would be used only for the management of COVID-19 and for no other purpose unless there was a "legal requirement", a phrase the policy documents nowhere define.[14] The terms of

---

[6] *Aarogya Setu FAQs*, AAROGYA SETU, https://www.aarogyasetu.gov.in/faq/ [https://web.archive.org/web/20200725171128/https://aarogyasetu.gov.in/faq/] (last visited Mar. 3, 2023); *see also* Matthan, *supra* note 2; Dar & Wani, *supra* note 1.

[7] Press Trust of India, *Go Corona Go, 'Sampark-o-Meter' Apps Developed by IISc, IITs to Fight against COVID-19*, HINDUSTAN TIMES (Apr. 9, 2020).

[8] Matthan, *supra* note 2; *Aarogya Setu FAQs*, *supra* note 6.

[9] Matthan, *supra* note 2; *see also Aarogya Setu Privacy Policy*, AAROGYA SETU, https://static.swaraksha.gov.in/privacy/ (last visited Mar. 3, 2023).

[10] *Aarogya Setu's Data Access and Knowledge Sharing Protocol, 2020*, VIDHI CENTRE FOR LEGAL POLICY (May 11, 2020), https://vidhilegalpolicy.in/blog/aarogya-setus-data-access-and-knowledge-sharing-protocol-2020/ (last visited Mar. 15, 2023).

[11] Matthan, *supra* note 2.

[12] *Our Concerns with the Aarogya Setu App*, SFLC.IN (Apr. 8, 2020), https://sflc.in/our-concerns-aarogya-setu-app/ (last visited Mar. 10, 2023).

[13] *Our Concerns with the Aarogya Setu App*, *supra* note 12.

[14] Dar & Wani, *supra* note 1; *Our Concerns with the Aarogya Setu App*, *supra* note 12.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

service, moreover, exempted the Government from liability for unauthorised access to users' information, leaving it without liability even if users' personal data leaked.[15]

### B. Location tracking, geofencing and mandatory quarantine enforcement

The World Health Organization advised that a COVID-19 patient be kept in isolation until ten days after symptom onset plus at least three days without symptoms or, for an asymptomatic case, until ten days after a positive test.[16] In parallel with contact tracing, several State governments put in place invasive monitoring systems to enforce home quarantine. Tamil Nadu's COVID-19 Quarantine Monitor, Karnataka's Quarantine Watch,[17] Goa's COVID-Locator[18] and Maharashtra's MahaKavach[19] relied on GPS tracking, periodic geotagged selfies, or both, to verify compliance. In Delhi, authorities had telecom companies locate quarantined individuals through cell-tower data in order to monitor their movements.[20] Although these applications relied on terms of service and voluntary downloads to imply consent, practical enforcement mechanisms, such as mandatory location tracking, periodic selfie uploads and alerts sent to local authorities upon non-compliance, effectively compelled participation. On this view, consent was not truly voluntary, which casts doubt on whether such surveillance met the constitutional requirement of legality. Methods such as cell-tower tracking, moreover, left individuals no alternative but to be monitored, at times without their explicit knowledge or permission.[21]

### C. Data leakages, stigmatisation and systemic vulnerabilities

The absence of uniform security standards led to widespread data spillage and privacy violations. Dar and Wani report that India saw some of its largest health data breaches in 2022, when the COVID-19 data of lakhs of citizens, uploaded by district health authorities to their websites, was found online.[22] Authorities in Karnataka and elsewhere published lists of persons

---

[15] *Our Concerns with the Aarogya Setu App*, *supra* note 12.
[16] WORLD HEALTH ORGANIZATION, *Criteria for Releasing COVID-19 Patients from Isolation* (June 17, 2020), https://www.who.int/news-room/commentaries/detail/criteria-for-releasing-covid-19-patients-from-isolation.
[17] *Karnataka, Tamil Nadu Monitoring COVID-19 Quarantines Through App*, BUSINESS STANDARD (Mar. 29, 2020), https://www.business-standard.com/article/pti-stories/karnataka-tamil-nadu-monitoring-covid-19-quarantines-through-app-120032900841_1.html.
[18] Press Trust of India, *Goa Govt Launches 'COVID-Locator' App to Track Home Quarantine People*, HINDUSTAN TIMES (Apr. 5, 2020).
[19] *Coronavirus: 'MahaKavach' App to Help in Contact Tracing*, BUSINESS STANDARD (Apr. 1, 2020), https://www.business-standard.com/article/pti-stories/coronavirus-mahakavach-app-to-help-in-contact-tracing-120040101524_1.html; *see also* Matthan, *supra* note 2 (describing the Tamil Nadu, Karnataka and Maharashtra systems).
[20] *Covid-19 Update: Inspired by Singapore, Delhi to Track Mobile Phones to Enforce Quarantine*, HINDUSTAN TIMES (Apr. 1, 2020), https://www.hindustantimes.com/india-news/covid-19-police-told-to-track-mobile-phones-of-people-under-quarantine-says-delhi-cm/story-2sZ90oirpjMrKbjnG1KNRI.html (last visited Mar. 8, 2026); Matthan, *supra* note 2.
[21] Matthan, *supra* note 2.
[22] Dar & Wani, *supra* note 1.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

in home quarantine with their home addresses and travel histories, which were then circulated through messaging applications.[23] Such disclosures were followed by social stigmatisation, public harassment and targeted discrimination against vulnerable communities.[24] In another incident, the personal data and COVID-19 test results of thousands of people, reportedly drawn from a government server, were put up for sale on an online forum.[25] These lapses reveal a structural flaw: when health surveillance is implemented without robust statutory safeguards, data collection quickly expands beyond its original public health mandate.

These incidents took place before the Digital Personal Data Protection Act, 2023 was brought into force. They were governed, if at all, by the IT Act, the 2011 Rules and the constitutional standard laid down in *Puttaswamy*. They nonetheless remain a useful benchmark for assessing whether the DPDP Act remedies these specific vulnerabilities. The question for the next Part is whether the new statute would have prevented, or at least meaningfully constrained, the conduct described, and whether it offers adequate regulation to prevent such harm in a future health crisis.

## III. Legal Framework for Digital Data Protection

Data protection refers to the rules and regulations that limit how personal information capable of identifying an individual may be used. No one in a civilised society should have to fear that their privacy will be violated or their personal information exploited.[26] During a pandemic, the confidentiality of health information is critical: it is needed to check the unrestricted circulation of personal details and to secure isolation and a dignified life free from public disruption and interference.[27] The collection and use of health information must therefore respect individuals' privacy. In confronting a pandemic, the modern State is expected to protect individual privacy, of which health information is a vital part. Privacy lies at the core of individual freedom and is a vital value in contemporary society.[28]

---

[23] Aroon Deep, *Karnataka Govt Publishes Addresses of People in COVID-19 Quarantine*, MEDIANAMA (Mar. 26, 2020), https://www.medianama.com/2020/03/223-privacy-karnataka-addresses-coronavirus-quarantine/ (last visited Mar. 23, 2026); Dar & Wani, *supra* note 1.

[24] Lauren Frayer, *Blamed for Coronavirus Outbreak, Muslims in India Come Under Attack*, NPR (Apr. 23, 2020), https://www.npr.org/2020/04/23/839980029/blamed-for-coronavirus-outbreak-muslims-in-india-come-under-attack (last visited Mar. 21, 2026); Dar & Wani, *supra* note 1.

[25] Press Trust of India, *Covid-19 Related Data of Thousands of Indians Leaked Online*, INDIAN EXPRESS (Jan. 21, 2022).

[26] Dar & Wani, *supra* note 1.

[27] Dar & Wani, *supra* note 1.

[28] Dar & Wani, *supra* note 1; *see also* Marcello Ienca & Effy Vayena, *On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic*, 26 NATURE MED. 463 (2020), https://www.nature.com/articles/s41591-020-0832-5 (last visited Mar. 22, 2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

In India, early Supreme Court rulings such as *M.P. Sharma v. Satish Chandra*[29] and *Kharak Singh v. State of U.P.*[30] contained observations that the Constitution does not protect a right to privacy. In *Gobind v. State of M.P.*,[31] a three-judge Bench, drawing on the minority view in *Kharak Singh*, proceeded on the footing that a right to privacy could be located in Article 21 of the Constitution. The existence and extent of the right to privacy were determined authoritatively only when a nine-judge Bench was convened in *K.S. Puttaswamy (Retd.) v. Union of India*.[32] The Supreme Court in *Puttaswamy* not only unanimously upheld the right to privacy but also examined its history, scope and potential limitations. While this paper cannot offer an in-depth analysis of the *Puttaswamy* verdict or of the law of privacy, a brief summary may be of use.

The ruling found that privacy is a constitutionally protected right which "emerges primarily from the guarantee of life and personal liberty in Article 21", with elements also arising from the other facets of freedom and dignity guaranteed by Part III. To be left alone and to have one's personal space respected is a fundamental human right. Because privacy is part of human dignity, it is "not lost or surrendered merely because the individual is in a public place". The right to privacy extends to the confidentiality of personal information. Most crucially, the Court reasoned that, like other fundamental rights, privacy has limits; an infringement of privacy, however, must be authorised by a law that is itself just, fair and reasonable. The plurality opinion set a three-fold requirement for any action that infringes the right to privacy: "(i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them".[33]

The plurality opinion in *Puttaswamy* confirms that the right to privacy protects sensitive information such as medical records: an "unauthorised parting of the medical records of an individual which have been furnished to a hospital will amount to an invasion of privacy". The Court used medical records to illustrate the balance to be struck between people's right to privacy and the State's legitimate interest in their personal data. The Court observed that the

[29] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
[30] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295.
[31] *Gobind v. State of M.P.*, (1975) 2 SCC 148.
[32] *Puttaswamy*, *supra* note 4; Vipul Kharbanda, *Government's COVID-19 Responses in the Context of Privacy: Part I*, CENTRE FOR INTERNET AND SOCIETY (Sept. 24, 2020), https://cis-india.org/internet-governance/blog/government2019s-covid-19-responses-in-the-context-of-privacy-part-i [https://web.archive.org/web/20240417113656/https://cis-india.org/internet-governance/blog/government2019s-covid-19-responses-in-the-context-of-privacy-part-i] (last visited Mar. 15, 2026).
[33] *Puttaswamy*, *supra* note 4 (Chandrachud, J., for himself, Khehar, C.J., Agrawal and Nazeer, JJ.); Kharbanda, *supra* note 32.

State may have a legitimate interest in studying hospital data to understand and respond to an epidemic such as malaria or dengue, and that "[i]f the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it".[34]

During the pandemic, the Kerala High Court considered the Kerala Government's engagement of Sprinklr, a United States company, to process COVID-19 data. In an interim order of April 2020, it directed the State to anonymise all the data collected before Sprinklr could access it and to obtain the informed consent of individuals to the processing of their data by a foreign third party. It restrained Sprinklr from breaching the confidentiality of the data, from exploiting it commercially and from disclosing it to any third party, and directed that Sprinklr return the data once its contractual obligations ended and immediately delete any residual or secondary data it held.[35]

### A. The Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Any programme that focuses on health should respect people's liberty, equality and privacy. Notwithstanding the Supreme Court's recognition of the right to privacy, the protection of personal data in India has lagged behind.[36] The relevant instruments are the IT Act and the 2011 Rules.

The IT Act provides for both civil and criminal consequences for the unauthorised disclosure and misuse of personal data. Section 43A makes a body corporate that possesses, deals with or handles sensitive personal data or information, such as patient information, in a computer resource liable to pay compensation to any person affected where it is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain.[37] Breaches of confidentiality and privacy are punishable under section 72 of the IT Act: any person who, having secured access to an electronic record or other material in pursuance of powers conferred under the Act or the rules made under it, discloses it to another person without the consent of the person concerned may be punished with imprisonment for up

[34] *Puttaswamy*, *supra* note 4 (Chandrachud, J.); Kharbanda, *supra* note 32.
[35] Manu Sebastian, *Kerala HC Restrains Sprinklr From Breaching Data Confidentiality; Govt. Directed to Anonymize Data & Take Informed Consent*, LIVELAW (Apr. 24, 2020), https://www.livelaw.in/news-updates/kerala-hc-restrains-sprinklr-from-breaching-data-confidentiality-govt-directed-to-anonymize-data-take-informed-consent-155718 (last visited Mar. 18, 2026).
[36] Dar & Wani, *supra* note 1.
[37] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), § 43A [hereinafter IT Act].

to two years, a fine of up to Rs 1,00,000, or both.[38] An exception to the general rule of privacy and confidentiality is found in section 69 of the Act, which allows the Central or a State Government, if satisfied that it is necessary or expedient to do so "in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence", to direct any agency by order to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource.[39] Data in any computer resource, including private information, may therefore be intercepted, monitored or decrypted under this provision.

The 2011 Rules protect sensitive personal data or information (SPDI) handled by a body corporate, that is, a company, firm or other association of individuals engaged in commercial or professional activities. SPDI under the 2011 Rules includes information on physical, physiological and mental health condition and medical records and history,[40] information of the kind gathered by public health authorities and enterprises during the pandemic. Rule 4 requires a body corporate, and any person who collects, receives, possesses, stores, deals with or handles information on its behalf, to provide and publish a privacy policy for handling personal information, including SPDI.[41] Rule 6 requires the prior permission of the provider of the information before SPDI is disclosed to a third party, unless the disclosure has been agreed by contract or is necessary to comply with a legal obligation, and subject to a proviso for Government agencies mandated under law to obtain such information; a body corporate may not publish SPDI, and a third party that receives it may not disclose it further.[42] A body corporate that fails to maintain reasonable security practices may be liable to pay compensation to the person affected under section 43A of the IT Act.[43]

The Supreme Court has recognised the right to informational privacy as a fundamental right, but, as Goyal argues, the framework of the 2011 Rules was "wholly inadequate" to prevent harm to data principals. In her assessment it fell short on four counts: first, it treated privacy as a statutory rather than a fundamental right and did not apply to processing of personal data by the government; second, it took a narrow view of the kinds of data that need protection; third,

[38] IT Act § 72.
[39] IT Act § 69(1).
[40] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, GAZETTE OF INDIA, pt. II sec. 3(i) (Apr. 11, 2011), r. 3 [hereinafter 2011 Rules].
[41] 2011 Rules, r. 4.
[42] 2011 Rules, r. 6.
[43] IT Act § 43A.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

it placed few obligations on data fiduciaries, and those could be overridden by contract; and fourth, it attached only minimal consequences to a fiduciary's breach of those obligations.[44]

This framework is transitional. The Digital Personal Data Protection Act, 2023 provides for the omission of section 43A of the IT Act,[45] but that provision, like the Act's substantive obligations, is not due to commence until May 13, 2027. Until then, the IT Act and the 2011 Rules, with the limitations discussed above, continue to govern the processing of health data by private entities.

Further, the binding Code of Ethics issued by the Medical Council of India is silent on how health data is treated once it is disclosed to the government, and it does not provide for anonymisation. The Electronic Health Record Standards provide for the anonymisation of personal data where disclosure is required, including for national priorities such as communicable diseases, and they require audit logs and restricted access. The Standards, however, remain within the IT Act framework, which does not apply to the government, and so cannot address the accountability of government entities.[46]

The 2011 Rules offer only a minimal framework for data security, and public bodies were not obliged to safeguard data during the public health crisis, leaving the information of millions of people at risk. Dar and Wani stress that individual liberty must be upheld while the health crisis is tackled. They argue that, although data can be used for good, "the arbitrary and uncontrolled use of data, particularly personal data, has raised questions about an individual's privacy and autonomy", and that collecting and disseminating personal data without consent in the absence of a data protection law is dangerous. The government defended the dissemination of such information as essential to containing the outbreak; Dar and Wani respond that publishing personal details pushed people away when their cooperation was needed to fight the disease together.[47]

---

[44] Trishee Goyal, *A First Look at the New Data Protection Bill*, THE HINDU (Nov. 20, 2022), https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece.

[45] The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023), § 44(2) [hereinafter DPDP Act]; MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), cl. (c) (Nov. 13, 2025); *see also* The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), GAZETTE OF INDIA, pt. II sec. 3(i) (Nov. 13, 2025), r. 1 [hereinafter DPDP Rules].

[46] Trishi Jindal, *India's COVID-19 Response Calls for Urgent Data Disclosure Norms*, VIDHI CENTRE FOR LEGAL POLICY (Apr. 29, 2020), https://vidhilegalpolicy.in/blog/indias-covid-19-response-calls-for-urgent-data-disclosure-norms (last visited Mar. 24, 2023).

[47] Dar & Wani, *supra* note 1.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

### B. The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025

The DPDP Act received presidential assent on August 11, 2023.[48] It applies to digital personal data, including data collected offline and later digitised, and to processing outside India that is connected with offering goods or services to individuals in India.[49] It is being brought into force in stages: the provisions establishing the Data Protection Board and the amendment to the Right to Information Act, 2005 took effect on November 13, 2025, while the provisions on grounds of processing, notice, consent, fiduciary obligations, rights, exemptions and penalties are due on May 13, 2027.[50] The DPDP Rules supply the procedural detail. The Act matters for this paper because it is the first general statute that would bind the State, as well as private entities, when digital tools are deployed in a health emergency. The question is whether it answers the concerns identified in Part II. In several respects it does. The principal gaps are set out below.

First, the Act does not treat health data as a distinct category. Personal data is defined simply as data about an identifiable individual,[51] and the category of sensitive personal data, which included medical records under the 2011 Rules, is not carried forward; section 43A of the IT Act, on which that regime rests, is to be omitted when section 44(2) of the DPDP Act commences.[52] The only gradation is the power to notify Significant Data Fiduciaries by reference to factors that include the volume and sensitivity of the data processed.[53] Unless so notified, a State application holding names, addresses, symptoms and location trails is bound by the same baseline duties as any other fiduciary.[54]

Second, and most important here, section 7 permits processing without consent for listed "legitimate uses". These include responding to a medical emergency and taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or other threat to public health.[55] This supplies the legal footing that the pandemic-era applications lacked, but it leaves three gaps. (i) The wording is naturally read to cover testing, treatment and vaccination, and arguably contact tracing; it is not clearly apt for enforcement-

[48] DPDP Act (assented to by the President on Aug. 11, 2023).
[49] DPDP Act § 3(a)–(b).
[50] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, Notification G.S.R. 843(E) (Nov. 13, 2025), *reproduced in* DPDP Act, https://www.indiacode.nic.in/bitstream/123456789/22037/2/a2023-22.pdf (last visited Oct. 1, 2026).
[51] DPDP Act § 2(t); 2011 Rules, r. 3.
[52] DPDP Act § 44(2)(a).
[53] DPDP Act § 10(1)–(2); DPDP Rules, r. 13.
[54] *See* Paarth Naithani, *Protecting Healthcare Privacy: Analysis of Data Protection Developments in India*, 9 INDIAN J. MED. ETHICS 149 (2024), https://doi.org/10.20529/IJME.2023.078.
[55] DPDP Act § 7(f)–(g).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

oriented measures such as monitoring quarantine compliance, geo-fencing or publishing the names of quarantined persons. Such measures would have to rest on the separate ground of performance of a State function under any law,[56] which carries no health-specific limits. (ii) Section 7 contains no express requirement of necessity or proportionality, no sunset tied to the duration of the emergency and no standard of anonymisation. Commentators argue that the proportionality discipline of *Puttaswamy* has not been carried into the Act, although the Supreme Court required restrictions on individual autonomy during COVID-19 to be proportionate.[57] (iii) The DPDP Rules prescribe processing standards for State processing under section 7(b), which concerns benefits and services, and for research, but not for processing under section 7(c) or 7(g).[58]

Third, the transparency duties do not reach emergency processing. The notice under section 5 accompanies a request for consent and so does not apply where the State relies on section 7; the DPDP Rules require intimation to the data principal only for State processing under section 7(b).[59] Even where a notice is required, section 5 does not oblige the fiduciary to disclose the recipients of the data, retention periods or cross-border transfers, and on the text of rule 3 the DPDP Rules add no such requirement.[60] Part II showed that unclear disclosure was among the main failings of the pandemic applications.

Fourth, the rights of data principals may not reach emergency data. The rights of access and of correction, completion, updating and erasure are framed as rights against a fiduciary to whom the principal has previously given consent, including consent given by voluntarily providing data under section 7(a).[61] By their wording, they do not extend to data processed on the other legitimate-use grounds, which would include data collected under section 7(g). The rights of grievance redressal and nomination are not so limited.[62] Separately, processing by the State is exempt from the erasure duty in section 8(7) and from the right of erasure,[63] so the Act does not require a test result or quarantine record held by a public body to be deleted once the emergency has ended. Such records can lead to stigma and discrimination, and the Act gives data principals neither portability nor a right to object to profiling or automated decisions.[64]

---

[56] DPDP Act § 7(c).
[57] Shivangi Rai & Shefali Malhotra, *India Is Piloting Ambitious Digital Health Initiatives While Neglecting Data Safeguards*, SCROLL.IN (Oct. 31, 2023); on the Supreme Court's approach to restrictions on autonomy during COVID-19, *see Jacob Puliyel v. Union of India*, W.P. (C) No. 607 of 2021, ¶ 89(iii), (v) (SC May 2, 2022).
[58] DPDP Rules, r. 5(1) & Second Schedule (standards for processing under § 7(b) and § 17(2)(b) of the DPDP Act).
[59] DPDP Act § 5(1); DPDP Rules, r. 3 & Second Schedule, cl. (g).
[60] Rai & Malhotra, *supra* note 57.
[61] DPDP Act §§ 11(1), 12(1).
[62] DPDP Act §§ 13–14.
[63] DPDP Act §§ 8(7), 12(3), 17(4).
[64] Rai & Malhotra, *supra* note 57.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Fifth, the scope provisions leave two openings. The Act covers non-digital data only if it is subsequently digitised, so paper registers and manually maintained lists fall outside it until then.[65] More significantly, it does not apply to personal data made publicly available by the data principal or by a person who is legally obliged to make it public.[66] Where an authority publishes identifiable quarantine or patient information under a legal obligation, the Act may therefore cease to protect that information, even though Part II described the stigma and misuse that followed the publication of such lists.

Sixth, the State exemptions are wide, and nothing separates health data from enforcement use. The Central Government may notify any instrumentality of the State as wholly outside the Act on grounds that include the maintenance of public order;[67] processing in the interest of preventing, detecting, investigating or prosecuting any offence is exempt from most fiduciary obligations and from the rights chapter, although the duties of responsibility and security safeguards in sections 8(1) and 8(5) continue to apply;[68] and the Central Government may, within five years of commencement, declare that any provision shall not apply to specified fiduciaries.[69] During COVID-19, data collected for care and surveillance was also used to enforce quarantine and lockdown rules, and nothing in the Act prevents similar repurposing, since enforcement is itself an exempted purpose. Challenges to sections 17(1)(c) and 17(2) are pending before the Supreme Court.[70]

Seventh, the research exemption is thinly conditioned. Processing for research, archiving or statistical purposes falls outside the Act where the data is not used to take decisions about a particular data principal and the prescribed standards are followed.[71] Those standards address lawfulness, minimisation, accuracy, retention, security and accountability, but they do not require anonymisation or pseudonymisation, or review by an ethics committee. That matters because epidemiological research on emergency data is likely to be extensive. Health researchers have recommended pseudonymisation and ethics-committee approval before clinical data is reused for research.[72]

---

[65] DPDP Act § 3(a).
[66] DPDP Act § 3(c)(ii).
[67] DPDP Act § 17(2)(a).
[68] DPDP Act §§ 8(1), 8(5), 17(1)(c).
[69] DPDP Act § 17(5).
[70] Debby Jain, *'Some Creases To Be Ironed Out,' Supreme Court Refers Pleas Challenging DPDP Act Amendment To RTI Act To Larger Bench*, LIVELAW (Feb. 16, 2026), https://www.livelaw.in/amp/top-stories/supreme-court-refers-pleas-challenging-dpdp-act-amendment-to-rti-act-to-larger-bench-523266 (last visited Oct. 9, 2026); *Supreme Court Hearing: DPDP Act Challenges to RTI*, FOX MANDAL (Aug. 12, 2026), https://foxmandal.in/news/supreme-court-hearing-dpdp-act-challenges-to-rti/ (last visited Oct. 9, 2026).
[71] DPDP Act § 17(2)(b); DPDP Rules, r. 16 & Second Schedule.
[72] Anubhuti Sood et al., *Challenges and Recommendations for Enhancing Digital Data Protection in Indian Medical Research and Healthcare Sector*, 8 NPJ DIGIT. MED. 48 (2025) (Recommendation 3), https://doi.org/10

Eighth, the security regime is stronger than the remedies. The Act imposes a duty to take reasonable security safeguards and to intimate breaches to the Board and affected individuals, and the DPDP Rules add minimum safeguards and a two-stage reporting process.[73] These provisions would apply to leaks of the kind that occurred during the pandemic, with penalties of up to Rs 250 crore for a failure to take security safeguards.[74] However, penalties are imposed only for breaches that the Board finds significant and are credited to the Consolidated Fund of India, and the Act provides no compensation to the affected individual; commentators have criticised both points.[75] Section 39 also bars civil courts from entertaining matters within the Board's powers, which, read with the absence of a compensation provision, may leave a person harmed by a leak without a damages remedy under the Act, although section 38(1) preserves other laws.[76] The Act further protects the Central Government for acts done in good faith.[77]

Ninth, institutional safeguards depend on the Executive. The Board is established by the Central Government, which appoints the Chairperson and Members, prescribes their terms of service and may re-appoint them after a two-year term;[78] the Act describes the Board as independent but leaves the selection process to the Rules.[79] The Central Government may also call for information from the Board and from data fiduciaries, although the Rules confine this to listed purposes, one of which is State use of personal data for the performance of any function under law.[80] The Ministry invited applications for the Board in May 2026 and, as at October 2026, no appointments had been reported, and the Union told the Kerala High Court that the Board had been constituted but was not yet functional,[81] so the enforcement body had yet to function in practice. Since the State is likely to be the principal fiduciary in a health emergency, a body appointed and re-appointed by the same Executive may be poorly placed to scrutinise it. Accountability is also affected by the amendment of section 8(1)(j) of the Right to Information Act, which now exempts information relating to personal information without the qualifications

.1038/s41746-025-01448-x.

[73] DPDP Act § 8(5)–(6); DPDP Rules, rr. 6–7.

[74] DPDP Act, Schedule, Sl. No. 1.

[75] DPDP Act §§ 33(1), 34.

[76] DPDP Act §§ 38(1), 39.

[77] DPDP Act § 35.

[78] DPDP Act §§ 19(2), 20; DPDP Rules, rr. 17–18.

[79] DPDP Act § 28(1).

[80] DPDP Act § 36; DPDP Rules, r. 23 & Seventh Schedule.

[81] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, F. No. 2(1)/2026-Pers.I, *Appointment to the Post of Chairperson and Other Members in the Data Protection Board of India* (May 6, 2026), https://www.meity.gov.in/static/uploads/2026/05/cd481c027470b420b4cb85fb40a91c53.pdf (last visited Oct. 9, 2026); MIRVOLEGAL, *DPDP Rules, 2025: Compliance Timeline for Data Fiduciaries* (Sept. 20, 2026), https://www.mirvolegal.com/insights/dpdp-rules-2025-compliance-timeline/ (last visited Oct. 9, 2026); *C.R. Neelakandan v. Union of India*, WP(PIL) No. 15 of 2026 (Ker. HC) (India), *reported in* 2026 LiveLaw (Ker) 570, https://www.livelaw.in/high-court/kerala-high-court/kerala-high-court-digi-yatra-data-protection-board-553994 (last visited Oct. 29, 2026).

of the earlier clause; the general public-interest override in section 8(2) of that Act is untouched,[82] and the amendment is under challenge before the Supreme Court.[83]

On balance, the DPDP Act and Rules improve on the pandemic-era position by giving epidemic processing a statutory basis and by imposing security, breach-intimation and penalty provisions that apply to the State. For digital health surveillance, however, the gaps cluster in the broad section 7 ground, the absence of notice and rights for emergency data, the State exemptions, the thin remedies and the Board's dependence on the Executive. Because the principal obligations will not commence until May 2027, the IT Act and the 2011 Rules, with the limitations noted in Part III.A, remain the law in force until then.

## IV. Conclusion and Suggestions

The pandemic showed that health and privacy need not be traded against each other, and that temporary measures tend to outlast the emergencies that justify them. The Digital Personal Data Protection Act, 2023 and the Rules of 2025 improve on the position that obtained during the pandemic by giving epidemic processing a statutory basis and by imposing security and breach-intimation duties on the State as well as on private entities. For digital health surveillance, however, the protection remains incomplete. The section 7 ground carries no express proportionality limit, emergency data may fall outside the notice and rights provisions, the State exemptions are wide, remedies are thin and the Board depends on the Executive. These gaps can largely be closed through rules, binding protocols and, where necessary, amendment, guided by the *Puttaswamy* requirements of legality, necessity and proportionality. The following measures are suggested:

1. Public health authorities and the operators of national health or surveillance applications should be notified as Significant Data Fiduciaries under section 10, and rules should prescribe heightened safeguards for health data.
2. Section 7(g) should be amended, or a binding emergency protocol issued, requiring a published declaration of the threat, a defined list of data elements, purpose limitation, retention that ends with the declared emergency, and anonymised or aggregated data for analytics, with anonymisation criteria prescribed to prevent re-identification by triangulating data sets.

[82] DPDP Act § 44(3) (substituting clause (j) of § 8(1) of the Right to Information Act, 2005); *see also* Right to Information Act, 2005, § 8(2).
[83] *See* sources cited *supra* note 70.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

3. Each application should carry a public notice stating what is collected, why, who receives it and for how long it is kept, and the government should publish which agencies access the data and the terms on which private firms are engaged.
4. Sections 11 and 12 should extend, at least as to access and correction, to processing under sections 7(c), 7(f), 7(g) and 7(h), and the State's exemption from erasure should give way to a fixed retention schedule, including deletion of an individual's records once an application is uninstalled or the emergency ends.
5. Health data collected for public health should be shared for enforcement only under a written, reasoned and proportionate order subject to independent review; the exclusion for publicly available data should not cover health data published by authorities; and notifications under section 17(2)(a) should be published with reasons, with section 17(5) not used to relax obligations over health data.
6. Pseudonymisation and ethics-committee approval should be conditions of the research exemption in section 17(2)(b) for health data.
7. The Board should be empowered to direct compensation to affected individuals, the relationship between section 39 and other remedies should be clarified, public health platforms should undergo independent security testing, and private processors should be bound by contract to the Act's security and erasure obligations.
8. Board members should be selected through an independent committee for longer, non-renewable terms, the Board should report annually to Parliament, and aggregate information on emergency data practices should be published proactively so that scrutiny does not depend on RTI requests.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]