Centre
for Internet
& Society

Do We Need a Separate Health Data Law in India?

Summary of roundtable discussions

February 6, 2025

By Pallavi Bedi and Shweta Mohandas

Copy Editing - The Clean Copy

Chapter 1. Background

Digitisation has become a cornerstone of India's governance ecosystem since the National e-Governance Plan (NeGP) of 2006. This trend can also be seen in healthcare, especially during the COVID-19 pandemic, with initiatives like the Ayushman Bharat Digital Mission (ABDM). However, the digitisation of healthcare has been largely conducted without legislative backing or judicial oversight. This has resulted in inadequate grievance redressal mechanisms, potential data breaches, and threats to patient privacy.

Unauthorised access to or disclosure of health data can result in stigmatisation, mental and physical harassment, and discrimination against patients. Moreover, because of the digital divide, overdependence on digital health tools to deliver health services can lead to the exclusion of the most marginalised and vulnerable sections of society, thereby undermining the equitable availability and accessibility of health services. Health data in the digitised form is also vulnerable to cyberattacks and breaches. This was evidenced in the recent ransomware attack on All India Institute of Medical Science, which, apart from violating the right to privacy of patients, also brought patient care to a grinding halt.

In this context, and with the rise in health data collection and uptick in the use of AI in healthcare, there is a need to look at whether India needs a standalone legislation to regulate the digital health sphere. It is also necessary to evaluate whether the existing policies and regulations are sufficient, and if amendments to these regulations would suffice.

This report discusses the current definitions of health data including international efforts, the report then proceeds to share some key themes that were discussed at three roundtables we conducted in May, August, and October 2024. Participants included experts from diverse stakeholder groups, including civil society organisations, lawyers, medical professionals, and academicians. In this report, we collate the various responses to two main aspects, which were the focus of the roundtables:

(1) In which areas are the current health data policies and laws lacking in India?

(2) Do we need a separate health data law for India? What are the challenges associated with this? What are other ways in which health data can be regulated?

Chapter 2. How is health data defined?

There are multiple definitions of health data globally. These include those incorporated into the text of data protection legislations or under separate health data laws. In the European Union (EU), the General Data Protection Regulation defines "data concerning health" as personal data that falls under special category data. This includes data that requires stringent and special protection due to its sensitive nature. Data concerning health is defined under Article(Article 4[15]) as "personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which

reveal information about his or her health status". The United States has the Health Insurance Portability and Accountability Act (HIPAA), which was created to make sure that the personally identifiable information (PII) gathered by healthcare and insurance companies is protected against fraud and theft and cannot be disclosed without consent. As per the World Health Organisation (WHO), 'digital health' refers to "a broad umbrella term encompassing eHealth, as well as emerging areas, such as the use of advanced computing sciences in 'big data', genomics and artificial intelligence".

2.1. Current legal framework for regulating the digital healthcare ecosystem in India

In India the digital health data had been defined under the draft Digital Information Security in Healthcare Act (DISHA), 2017, as an electronic record of health-related information about an individual. and includes the following: (i) information concerning the physical or mental health of the individual; (ii) information concerning any health service provided to the individual; (iii) information concerning the donation by the individual of any body part or any bodily substance; (iv) information derived from the testing or examination of a body part or bodily substance of the individual; (v) information that is collected in the course of providing health services to the individual; or (vi) information relating to the details of the clinical establishment accessed by the individual.

However, DISHA was subsumed into the 2019 version of the Personal Data Protection Act, called The Data and Privacy Protection Bill, which had a definition of health data and a demarcation between sensitive personal data and personal data. Both these definitions are absent from the Digital Personal Data Protection Act (DPDPA), 2023. This makes uncertain what is defined as health data in India. It is also important to note that the health data management policies released during the pandemic relied on the definition of health data under the then draft of the Personal Data Protection Act.

(i) Drugs and Cosmetic Act, and Rules

At present, there is no specific law that regulates the digital health ecosystem in India. The ecosystem is currently regulated by a mix of laws regulating the offline/legacy healthcare system and policies notified by the government from time to time. The primary law governing the healthcare system in India is the Drugs and Cosmetics Act (DCA), 1940, read with the Drugs and Cosmetic Rules, 1945. These regulations govern the manufacture, sale, import, and distribution of drugs in India. The central and state governments are responsible for enforcing the DCA. In 2018, the central government published the Draft Rules to amend the Drugs and Cosmetics Rules in order to incorporate provisions relating to the sale of drugs by online pharmacies (Draft Rules). However, the final rules are yet to be notified. The Draft Rules prohibit online pharmacies from disclosing the prescriptions of patients to any third person. However, they also mandate the disclosure of such information to the central and state governments, as and when required for public health purposes.

(ii) Clinical Establishments (Registration and Regulation) Act, and Rules

The Clinical Establishments Rules, 2012, which are issued under the Clinical Establishments (Registration and Regulation) Act, 2010, require clinical establishments to maintain electronic health records (EHRs) in accordance with the standards determined by the central government. The Electronic Health Record (EHR) Standards, 2016, were formulated to create a uniform standards-based system for EHRs in India. They provide guidelines for clinical establishments to maintain health data records as well as data and security measures. Additionally, they also lay down that ownership of the data is vested with the individual, and the healthcare provider holds such medical data in trust for the individual.

(iii) Health digitisation policies under the National Health Authority

In 2017, the central government formulated the National Health Policy (NHP). A core component of the NHP is deploying technology to deliver healthcare services. The NHP recommends creating a National Digital Health Authority (NDHA) to regulate, develop, and deploy digital health across the continuum of care. In 2019, the Niti Aayog, proposed the National Digital Health Blueprint (Blueprint). The Blueprint recommended the creation of the National Digital Health Mission. The Blueprint made this proposition stating that "the Ministry of Health and Family Welfare has prioritised the utilisation of digital health to ensure effective service delivery and citizen empowerment so as to bring significant improvements in public health delivery". It also stated that an institution such as the National Digital Health Mission (NDHM), which is undertaking significant reforms in health, should have legal backing.

(iv) Telemedicine Practice Guidelines

On 25 March 2020, the Telemedicine Practice Guidelines under the Indian Medical Council Act were notified. The Guidelines provide a framework for registered medical practitioners to follow for teleconsultations.

2.2. Digital Personal Data Protection Act, 2023

There has been much hope for India's data protection legislation in India to cover definitions of health data, keeping in mind the removal of DISHA and the uptick in health digitisation in both the public and private health sectors. The privacy/data protection law, the DPDPA was notified on 12 August 2023. However, the provisions have still not come into force. So, currently, health data and patient medical history are regulated by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules), 2011. The SPDI Rules will be replaced by the DPDA as and when its different provisions are enforced. On 3 January 2025, the Ministry of Electronics and Information Technology released the Draft Digital Personal Data Protection Rules, 2025, for public consultation. The last date for submitting the comments is 18 February 2025.

Health data is regarded as sensitive personal data under the SPDI Rules. Earlier drafts of the data protection legislation had demarcated data as personal data and sensitive personal data, and health data was regarded as sensitive personal data. However, the DPDA has removed the distinction between personal data and sensitive personal data. Instead, all data is regarded as personal data. Therefore, the extra protection that was previously afforded to health data has been removed. The Draft Rules also do not mention health data or provide any additional safeguards when it comes to protecting health data. However, it exempts healthcare professionals from the obligations that have been put on data fiduciaries when it comes to processing children's data. The processing has to be restricted to the extent necessary to protect the health of the child.

As seen so far, while there are multiple healthcare-related regulations that govern stakeholders – from medical device manufacturers to medical professionals – there is still a vacuum in terms of the definition of health data. The DPDPA does not clarify this definition. Further, there are no clear guidelines for how these regulations work with one another, especially in the case of newer technologies like AI, which have already started disrupting the Indian health ecosystem.

Chapter 3. Key takeaways from the health data roundtables

The three health data roundtables covered various important topics related to health data governance in India. The first roundtable highlighted the major concerns and examined the granular details of considering a separate law for digital healthcare. The second round table featured a detailed discussion on the need for a separate law, or whether the existing laws can be modified to address extant concerns. There was also a conversation on whether the absence of a classification absolves organisations from the responsibility to protect or secure health data. Participants stated that due to the sensitivity of health data, data fiduciaries processing health data could qualify it as significant data fiduciary under the the proposed DPDPA Rules (that were at the time of hosting the roundtables) yet to be published. The final roundtable concluded with an in-depth discussion on the need for a health data law. However, no consensus has emerged among the different stakeholders.

The roundtables highlighted that the different stakeholders – medical professionals, civil society workers, academics, lawyers, and people working in startups – were indeed thinking about how to regulate health data. But there was no single approach that all agreed on.

3.1. Health data concerns

Here, we summarise the key points that emerged during the three roundtables. These findings shed light on concerns regarding the collection, sharing, and regulation of health data.

(i) Removal of sensitive personal data classification

In the second roundtable, there was a discussion on the removal of the definition of health data from the final version of the DPDPA, which also removed the provision for sensitive personal data; health data previously came under this category. One participant stated that differentiating between sensitive personal data and data was important, as sensitive personal data such as health data warrants more security. They further stated that without such a clear distinction, data such as health status and sexual history could be easily accessed. Participants also pointed out that given the current infrastructure of digital data, the security of personal data is not up to the mark. Hence a clear classification of sensitive and personal data would ensure that data fiduciaries collecting and processing sensitive personal data would have greater responsibility and accountability.

(ii) Definition of informed consent

The term 'informed consent' came up several times during the roundtable discussions. But there was no clarity on what it means. A medical professional stated that in their practice, informed consent applies only to treatment. However, if the patient's data is being used for research, it goes through the necessary internal review board and ethics board for clearance. One participant mentioned that the Section 2(i) of the Mental Healthcare Act (MHA), 2017 defines informed consent as

> consent given for a specific intervention, without any force, undue influence, fraud, threat, mistake or misrepresentation, and obtained after disclosing to a person adequate information including risks and benefits of, and alternatives to, the specific intervention in a language and manner understood by the person; a nominee to make a decision and consent on behalf of another person.

Neither the DPDA nor the Draft DPDPA Rules define informed consent. However, the Draft DPDA Rules state that the notice given by the data fiduciary to the data principal must use simple, plain language to provide the data principal with a full and transparent account of the information necessary so that they can provide informed consent to process their personal data.

A stakeholder pointed out that consent is taken without much nuance or the option for choice or nuance. Indeed, consent is often presented in non-negotiable terms, creating power imbalances and undermining patient autonomy. Suggested solutions include instituting granular and revocable consent mechanisms. This point also emerged during the third roundtable, where it was highlighted that consenting to a medical procedure was different from consenting to data being used to train AI. When a consent form that a patient or caregiver is asked to sign gives the relevant information and no choice but to sign, it creates a severe power imbalance. Participants also emphasised that there was a need to assess if consent was being used as a tool to enable more data-sharing or a mechanism for citizens to be given other rights, such as the reasonable expectation that their medical information would not be used for commercial interests, especially to their

own detriment, just because they signed a form. One suggested way to tackle this is for there to be greater demarcation of the aspects a person could consent to. This would give people more control over the various ways in which their data is used.

(iii) Data sharing with third parties

Discussions also focused on the concerns about sharing health data with third parties, especially if the data is transferred outside India. Data is/can be shared with tech companies and research organisations. So the discussions highlighted the regulations and norms governing how such data sharing occurs despite the fragmented regulations. For instance:

- Indian Council of Medical Research (ICMR) Ethical guidelines for application of Artificial Intelligence in Biomedical Research and Healthcare mandate strict protocols for sharing health data, but these are not binding. They state that the sharing of health data by medical institutions with tech companies and collaborators, must go through the ICMR and Health Ministry's Screening Committee. This committee has strict guidelines on how and how much data can be shared and how it needs to be shared. The process also requires that all PII is removed and only 10 percent of the total data is permitted to be shared with any collaborator outside of any Indian jurisdiction.
- Companies working internationally have to comply with global standards like the GDPR and HIPAA, highlighting the gaps in India's domestic framework which leaves the companies uncertain of which regulations to comply with. There is a need to balance the interests of startups that require more data and better longitudinal health records, and the need for strong data protection, data minimisation, and storage limitation.

(iv) Inadequate healthcare infrastructure

With respect to the implementation challenges associated with health data laws, participants noted that, currently, the Indian healthcare infrastructure is not up to the mark. Moreover, smaller and rural hospitals are not yet on board with health digitisation and may not be able to comply with additional rules and responsibilities. In terms of capacity as well, smaller healthcare facilities lack the resources to implement and comply with complex regulations.

3.2. Regulatory challenges

Significant time was spent on discussing the regulatory challenges and deficiencies in India's healthcare infrastructure. The discussion primarily revolved around the following points:

(i) State vs. central jurisdiction

Under the Constitutional Scheme, legislative responsibilities for various subjects are demarcated between the centre and the states, and are sometimes shared between them. The topics of public health and sanitation, hospitals, and dispensaries fall under the state list set out in the Seventh Schedule of the Constitution. This means that state governments have the primary responsibility of framing and implementing laws on these subjects. Under this, local governance institutions, namely local bodies, also play an important role in discharging public health responsibilities.

(ii) Do we bring back DISHA?

During the conversation about the need for the health data regulation, participants brought up that there had been an earlier push for a health data law in the form of DISHA, 2017. But this was later abandoned. DISHA aimed to set up digital health authorities at the national and state levels to implement privacy and security measures for digital health data and create a mechanism for the exchange of electronic health data.

Another concern that arose with respect to having a central health data legislation was that, as health is a state subject, there could be confusion about having a separate, centralised regulatory body to oversee how the data is being handled. This might come with a lack of clarity on who would address what, or which ministry (in the state or central government) would handle the redressal mechanism.

3.3. Are the existing guidelines enough?

Participants highlighted that enacting a separate law to regulate digital health would be challenging, considering that the DPDPA took seven years to be enacted, the rules are yet to be drafted, and the Data Protection Board has not been established. Hence, any new legislation would take significant resources, including manpower and time.

In this context, there were discussions acknowledging that although the DPDPA does not currently regulate health data, there are other forms of regulation and policies that are prescribed for specific types of interventions when it comes to health data; for example, the Telemedicine Practice Guidelines, 2020, and the Medical Council of India Rules. These are binding on medical practitioners, with penalties for non-conforming, such as the revoking of medical licenses. Similarly the ICMR guidelines on the use of data in biomedical research include specific transparency measures, and existing obligations on health data collectors that would work irrespective of the lack of distinction between sensitive personal data and personal data under the DPDPA.

However, another participant rightly pointed out that the ICMR guidelines and the policies from the Ministry of Health and Family Welfare are not binding. Similarly, regulations like the Telemedicine Practice Guidelines and Indian Medical Council Act are only applicable to medical practitioners. There are now a number of companies that collect and process a lot of health data; they are not covered by these regulations.

Although there are multiple regulations on healthcare and pharma, none of them cover or govern technology. The only relevant one is the Telemedicine Practice Guidelines, which say that AI cannot advise any patient; it can only provide support.

Chapter 4. Recommendations

Several key points were raised and highlighted during the three roundtables. There were also a few suggestions for how to regulate the digital health sphere. These recommendations and points can be classified into short-term measures and long-term measures.

4.1. Short-term measures

We propose two short-term measures, as follows:

(i) Make amendments to the DPDPA

Introduce sector-specific provisions for health data within the existing framework. The provisions should include guidelines for informed consent, data security, and grievance redressal.

(ii) Capacity-building

Provide training for healthcare providers and data fiduciaries on data security and compliance.

4.2. Long-term measures

We offer six long-term measures, as follows:

(i) Standalone legislation

Enact a dedicated health data law that

- Defines health data and its scope;
- Establishes a regulatory authority for oversight; and
- Includes provisions for data sharing, security, and patient rights.

(ii) National Digital Health Authority

Establish a central authority, similar to the EU's Health Data Space, to regulate and monitor digital health initiatives.

(ii) Cross-sectoral coordination

Develop mechanisms to align central and state policies and ensure seamless implementation.

(v) Technological safeguards

Encourage the development of AI-specific policies and guidelines to address the ethics of using health data.

(vi) Stringent measures to address data breaches

Increase the trust of people by addressing data breaches, and fostering proactive dialogue between patients, medical community, government and civil society. Reduce the exemption for data processing, such as that granted to the state for healthcare

Conclusion

The roundtable discussions highlighted the fragmented nature of the digital health sphere, and the issues that emanate from such a fractured polity. Considering the variations in the healthcare infrastructure and budget allocation across different states, the feasibility of enacting a central digital health law requires more in-depth research. The existing laws governing the offline/legacy health space also need careful examination to understand whether amendments to these laws are sufficient to regulate the digital health space.