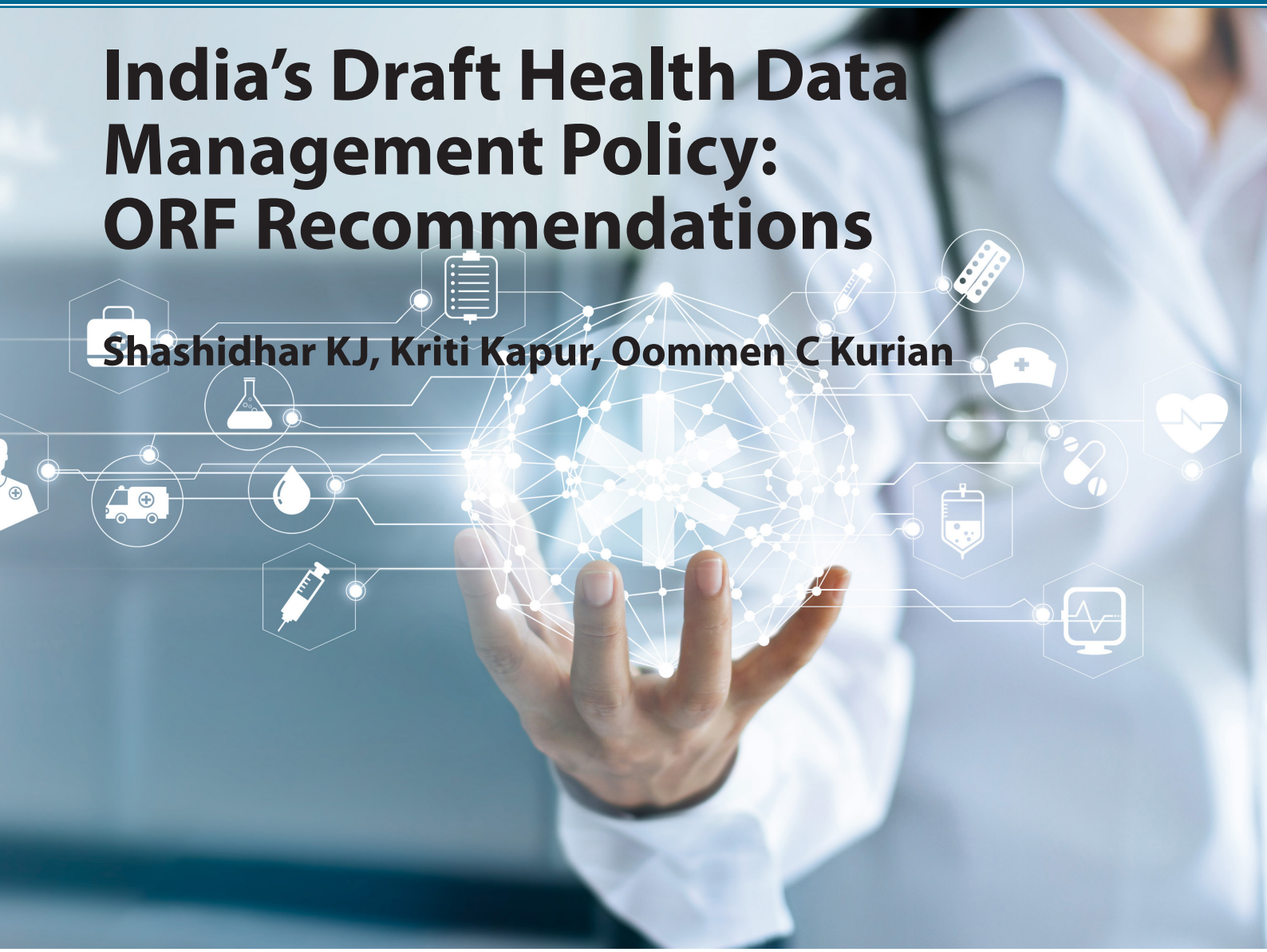
122

ORF SPECIAL REPORT

November 2020

India's Draft Health Data Management Policy: ORF Recommendations

Shashidhar KJ, Kriti Kapur, Oommen C Kurian



Getty Images Plus/ipopba

Attribution: Shashidhar KJ, Kriti Kapur, Oommen C Kurian, "India's Draft Health Data Management Policy: ORF Recommendations," *ORF Special Report No. 122*, November 2020, Observer Research Foundation.

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence the formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions.

To know more about ORF scan this code

INTRODUCTION

The COVID-19 pandemic has served as a wakeup call to India, as it has across the globe. Public health systems, both in developed and developing nations, are showing signs of stress in handling the number of patients afflicted by both COVID-19 and non-COVID ailments. As efforts to manage the pandemic tend to undermine care for other illnesses, including serious ones like cancer, there are concerns of delay in the diagnosis and treatment of these non-COVID illnesses.[1] Moreover, physical-distancing norms, as well as fear of contracting COVID-19 from a hospital, are preventing people from getting medical help in-person. The imperative is to build a comprehensive telemedicine network that will fill the gaps. Broadly, any telemedicine framework needs to provide the following services:

Building trust and consent: Telemedicine, by its very nature, upends the traditional doctor-patient relationship, which relies on in-person consultations. Telemedicine might act as a barrier to establishing trust with patients and, thus, may take informed consent away from patients when it comes to medical procedures.

Privacy and security: Privacy has been encoded into medical ethics from the time of Hippocrates and is bolstered by modern medical codes. However, telemedicine opens up opportunities for malicious operators who can breach security systems and compromise patient information. Health data requires the highest set of privacy and security safeguards. Systems must be put in place to ensure patient privacy and data security, along with a robust consent framework. Above all, there is a need to adopt a citizen-first approach when sharing health data.

Licensure and insurance: As increasing numbers of doctors and medical professionals populate telemedicine platforms from across different geographies, it is important to ensure that there are uniform licensure and accreditation standards for doctors who intend to practice telemedicine, regardless of their geographical location. Frameworks for insurance coverage for consultations through telemedicine should also be put in place.

The Government of India has been active in setting protocols for the adoption of telemedicine and published its Telemedicine Practice Guidelines in March 2020 towards better healthcare access and affordability.[2] Against this backdrop, the Ministry of Health and Family Welfare (MoHFW) initiated a public consultation in August 2020, inviting comments on the draft Health Data Management Policy of the National Digital Health Mission,

which intends to build a federated health data management infrastructure that ensures interoperability and transferability of health data within the National Digital Healthcare ecosystem.[3] The rest of this special report outlines ORF's submission in response to the call for comments.

Need for a Comprehensive Data Protection Framework

1. A robust Personal Data Protection Act should precede the Health Data Management Policy (HDMP). HDMP constitutes a vision document, outlining the minimum standards for data privacy and protection of health data for those who consent to share the same, and should be astutely aligned with the law. A standalone health data management policy without the legal support of a data protection law does not provide the necessary protection to the sensitive and private information that will be shared by citizens.

2. There has been a precedent for the creation of standalone data sharing policies by other ministries without the protections of the Personal Data Protection Act. For example, the Ministry of Road Transport and Highways (MoRTH) called for the digitisation and bulk sharing of data to private entities from the Vahan and Sarathi databases, which housed vehicle registration and drivers' license information. Without adequate privacy and security protections, there is potential for this data to be misused.[4] During the February 2020 riots in North East Delhi, for instance, there were reports that the Vahan database was used to target vehicles belonging to Muslims.[5] This led to the MoRTH scrapping this data sharing policy due to privacy concerns. Following the Independence Day address by Prime Minister Narendra Modi, the MoHFW piloted a programme in six union territories for the creation of the Health ID as prescribed by the HDMP; 55,000 IDs have been created as of the time of writing this report.[6] Given the sensitivity of health data, the MoHFW would be wise in pausing this pilot till a comprehensive Personal Data Protection Act is passed with relevant and widespread stakeholder participation.

Adopting a Citizen-First Approach

3. The policy should, above all, adopt a citizen-first approach while implementing various parts of the National Digital Health Ecosystem (NDHE), given the highly sensitive nature of the health data of data principals that will be shared with Health Information Providers (HIPs) and Health Information Users (HIUs). While the HDMP does elaborate

on the rights of digital principals—such as right to confirmation and access, and the right to correction and erasure—it does not make adequate provisions in case of disputes with data fiduciaries. The policy mentions that if these requests for information are rejected, it will give the data principal the reasons for refusal, and if the principal is dissatisfied with the outcome, "it may require the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal." The Personal Data Protection Bill also has guidelines for the appointment of Adjudicating Officers and the setting up of appellate tribunals to settle these disputes.

4. As part of the citizen-first approach, the HDMP must answer the questions, 'Who owns the data?' and 'Who has access to the data?' While the draft policy states that no data will be collected without prior consent, it does not adequately clarify who the owner of this data is, or who will have access to this data (whether the Centre, state, medical care providers, private institutions, among others). This also raises the question of how consent management will be monitored.

Penalties and compensation for non-compliance

5. The draft policy fails to explicitly mention the penalties and compensations for non-compliance with the policy or for offences like re-identification and processing of de-identified personal data, other than suspension or cancellation from participating in the NDHE. The Personal Data Protection Bill provides that individuals and officers in companies who do not comply with the law would be liable to imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees, or both.

6. The draft policy mentions that a data fiduciary can appoint a data protection officer as the grievance officer. The policy is looking to merge the offices of the data protection officer and the grievance officer, a divergence from the Personal Data Protection Bill, where these offices are separate. This sets up a power asymmetry between the data principal and the data fiduciary when seeking a redressal, where data principals will have a more difficult time seeking justice during disputes.

Framework to govern consent

7. The governing principles for the consent framework for data fiduciaries under HMDP have not been adequately elaborated. The draft policy

only mentions that data fiduciaries must make use of "appropriate technological means" to prevent security breaches and guarantee that access is given by data principals. It mentions that the "technical design of the consent management framework should also ensure interoperability across all players of the NDHE". However, there is no clarity on how the flow of the consent framework will look like for data principals. The policy should provide a flowchart on how the consent framework will function.

8. The HDMP borrows the concept of the consent manager from the Personal Data Protection Bill. Consent managers were introduced to reduce "consent fatigue" of data principals, though how it will work in practice remains to be seen. According to the Personal Data Protection Bill, these professionals need to be registered with the Data Protection Authority (DPA). It is unclear as to what kind of qualifications individuals need to become a consent manager in the HDMP. Would doctors and health practitioners function as consent managers?

The problems of building infrastructure and removing redundancies

9. The kind of infrastructure that the National Digital Health Ecosystem (NDHE) assumes to be already in place may prove to be a bottleneck. The nature of the data to be collected requires physical infrastructure as well as human resources earmarked for health information management. Given the fund-starved nature of India's health system, this is going to be the single biggest challenge for any effort at digitisation of health records. Does India have a roadmap to ease the infrastructural and human resource bottlenecks in the health system?

10. The National Health Resources Repository (NHRR), launched by Government of India earlier, which aimed to be an integrated Health Informatics Platform that can provide reliable, accurate and relevant national health information has a strong overlap with what the NDHM tries to achieve through HDMP. However, there is no mention of the NHRR in the draft policy. How are these initiatives linked and how will redundancy be eliminated?

11. With national registries of health professionals planned, priority should be given to data de-duplication (or elimination of redundant data) to make the information robust and to reduce required storage capacity as well as to establish a source of truthful and factual information. Existing

professional registries are notorious for the same professional(s) getting registered in multiple states with rolls not being updated for years.

Health ID creation and handling of sensitive data

12. The HDMP calls for the creation of the Health ID, which will be verified by linking it to an individual's Aadhaar number. It mentions that if people are unable to authenticate a Health ID using Aadhaar, verification would be done through other means. The draft policy does not elaborate on what these other means would be.

13. The HDMP mentions that the Health ID will be collecting Electronic Health Records (EHR), Personal Health Records (PHR) and Electronic Medical Records (EMR). However, the scope of data collected by these records is enormous and can include sensitive personal data such as biometrics; physical, psychological and mental health data; intersex status; sexual orientation; sex life data; financial information; caste or tribe; and religious or political beliefs. These records that are collected might not fit the data minimisation principles and it will be difficult to set purpose limitations on them. The policy's mandate that data collected "should be for a specific, lawful and clear purpose identified" contradicts itself.

14. The NDHE can potentially pave the way for a data-driven approach to addressing caste, religion, gender, region and income disparities in healthcare outcomes across India. In the generally data-starved environment of health policy research, anonymised information available for Big Data analysis can change the way solutions are designed. However, over-collection of data, and the subsequent mistrust created could be a possible risk factor. For instance, in the US, mandatory collection of patients' race data at hospitals has resulted in studies that informed policy to address inequities; in a sector known to be lightly regulated in India, this may cause resistance. The policy document refers to the collection of data points such as financial details, physical and mental health, sex life, medical records, gender and sexuality, caste, religious and political beliefs, and genetic and biometric records. However, the policy is seemingly ambiguous about the uses of such in-depth data, which may lead to mistrust amongst citizens—as seen in the case of Aadhaar linkages with mobile phones and bank accounts.

15. There is a lack of clarity on how the sensitive data will be protected. The draft policy does not sufficiently address the question of exactly how the data collected will be protected, thereby endangering the privacy of patients while also casting doubts on the intentions of medical service providers. The policy needs to focus on the role of an effective regulator for securing the digital infrastructure to govern such data to ensure protection of sensitive information and to garner confidence in the system.

16. For any such wide-ranging initiative like the Centre-led National Digital Health Mission to succeed, health has to move from being a subject on the State list to the Concurrent list, where both the Centre and States will have the power to legislate on matters related to health. In addition, HDMP will need to be aligned with relevant legislation other than the Personal Data Protection Act, like the Right to Information Act and even state-level laws, given health is a State subject yet. To start with, a mapping of such legislations should be conducted.

17. Finally, HDMP will need to be available in languages other than English for any true stakeholder participation in its finalisation.

About the Authors

Shashidhar KJ is Associate Fellow at ORF, Mumbai. **Kriti Kapur** is Junior Fellow at ORF. **Oommen C Kurian** is Senior Fellow and Head of Health Initiative at ORF.

ENDNOTES

1 Mitu Sengupta and Asit Arora, "Protecting Cancer Care through the Covid-19 Crisis and its Aftermath," *ORF Issue Brief No. 391*, August 2020, Observer Research Foundation.

2 *Telemedicine Practice Guidelines,* Ministry of Health and Family Welfare of India, 25 March, 2020, Accessed 12 November, 2020, https://www.mohfw.gov.in/pdf/Telemedicine.pdf

3 *National Digital Health Mission: Health Data Management Policy,* Ministry of Health and Family Welfare of India, 25 August 2020, Accessed 12 November 2020, https://ndhm.gov.in/health_management_policy

4 Shashidhar K.J., "An Assessment of the Bulk Data Sharing Policy of the Ministry of Road Transport and Highways", *ORF Issue Brief No. 332*, December 2019, Observer Research Foundation.

5 Nishita Saluja, "Transport ministry to partially conceal names of vehicle owners on Vahan database", *The Economic Times*, 27 February 2020, https://economictimes.indiatimes.com/news/economy/policy/transport-ministry-to-partially-conceal-names-of-vehicle-owners-on-vahan-database/articleshow/74338287.cms

6 Sumi Sukanya Dutta, "Digital Health Mission: Over 55,000 IDs created", *The New Indian Express,* 29 August 2020, https://www.newindianexpress.com/nation/2020/aug/29/digital-health-mission-over-55000-ids-created-2189757.html

Ideas • Forums • Leadership • Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005.
E-mail: contactus@orfonline.org
Website: www.orfonline.org