INTERNET FREEDOM FOUNDATION

internetfreedom.in rohin@internetfreedom.in +91 11 41437971

By Email

To,
Sh. Vikram Pagaria,
Joint Director Coordination (NDHM),
National health Authority
3rd, 7th & 9th Floor, Tower-L,
Jeevan Bharati Building,
Connaught Place,
New Delhi, Delhi - 110001

Email : jd.coord@nha.gov.in

Dated: July 20th, 2021 **IFF/2021/074**

Re: Comments on consultation Paper on Healthcare Professionals Registry

Dear Sir,

1. Internet Freedom Foundation (IFF) is a registered charitable trust which advocates for people's rights over the internet across public institutions and the private sector.

2. We believe that the Health Facility Registry must be conducted along certain established principles of data protection. To this extent, we have attached our detailed analysis of the National Digital Health Mission's Health Data Management Policy to serve as a guideline for the implementation of a Healthcare Professionals Registry.

We remain at your disposal should you wish to discuss the matter any further.

Kind Regards,

Rohin Garg,
Associate Policy Counsel,
Internet Freedom Foundation,
rohin@internetfreedom.in

Analysing the NDHM Health Data Management Policy

Shefali Malhotra*, Rohin Garg** and Shivangi Rai***

Abstract

Propelled by the COVID-19 pandemic, the Prime Minister of India launched the National Digital Health Mission on 15 August 2020. The aim of the Mission is to improve capacities in the Indian healthcare system by creating a digital health ecosystem connecting different stakeholders from the public and private healthcare sector. A key aspect of the Mission is to establish digital health IDs and a digital health records system. In order to guide its implementation, the Government of India notified the *National Digital Health Mission: Health Data Management Policy (NDHM-HDMP)* in December 2020. In this paper, we aim to provide a broad overview of the NDHM-HDMP and highlight related legal, socio-economic and implementation issues. We analyse the NDHM-HDMP based on five criteria: (a) legal foundation and health system preparedness; (b) governance framework; (c) implications for individual consent and privacy; (d) risk of exclusions; and (e) concerns around access to health big data by private entities. We find that the NDHM-HDMP, in its present form, suffers from a weak legal foundation and inadequate preparatory groundwork; excessive delegation; a constricted digital consent and privacy framework; over-reliance on an *Aadhaar*-based authentication system; and, vague systems for anonymisation and de-identification, as well as complete absence of strict access control requirements for personal health data. We recommend that the identified shortcomings are addressed prior to the full scale roll out of the digital health ID and digital health records system, in order to meet the objectives of the National Digital Health Mission.

* Shefali Malhotra is Research Consultant with the Centre for Health Equity, Law and Policy, ILS Law College, Pune. She can be contacted at shefalimalhotra@c-help.org.

** Rohin Garg is Associate Policy Counsel with the Internet Freedom Foundation, New Delhi. He can be contacted at rohin@internetfreedom.in.

*** Shivangi Rai is Deputy Coordinator with the Centre for Health Equity, Law and Policy, ILS Law College, Pune. She can be contacted at shivangirai@c-help.org.

Table of Contents

1 Introduction 2

2 Background 5

3 Prerequisites to a digital health records system 7

3.1 Legal foundation 7

3.2 State capacity 8

4 Governance framework 11

5 Consent and confidentiality 15

6 Data privacy and security 18

7 Inclusion 21

8 Access to health big data by private entities 25

9 Conclusion 27

1 Introduction

On 15 August 2020, the Indian Prime Minister launched the National Digital Health Mission (NDHM), an ambitious plan to build a digital health ecosystem that connects different stakeholders in the healthcare sector, both public and private. A key aspect of the mission is to establish a Unique Health Identifier (UHID) system that issues a unique identification number for each individual (or entity), which links to the Electronic Health Record (EHR) of that individual (or entity).[1] EHRs are a longitudinal electronic version of patients' complete medical history (tests, diagnosis, treatment, prescriptions, etc.) that can be seamlessly and efficiently exchanged with healthcare providers, with the aim of facilitating health information exchange for patient care and secondary use, including research and healthcare planning. After the announcement, the National Health Authority (NHA) officially rolled out digital health IDs in the six union territories of India, on a pilot basis.[2] On 14 December 2020, the government approved the *National Digital Health Mission: Health Data Management Policy* (NDHM-HDMP), to guide the development of the UHID system, as well as facilitate the creation, storing, processing and sharing of individual EHRs.[3]

The UHID and EHRs have the potential of making healthcare more efficient, cost effective, and accessible; but also entail significant risks to the privacy, confidentiality and protection of personal health data; and exclusion and unfairness due to digital illiteracy. In order to make a successful transition from paper to a digital system, and minimise the risks associated with it, it is necessary to ensure health system and security environment preparedness to support the digitisation. A robust legal and regulatory framework that protects individual rights, through adequate enforcement, transparency and accountability mechanisms, is also imperative. Accordingly, the NDHM-HDMP, which will form the foundation of UHID and EHRs, should balance between establishing and maintaining the digital health system, as well as protecting and promoting individual privacy, autonomy and dignity. In this context, we analyse the NDHM-HDMP and find five significant shortcomings: weak legal foundation and inadequate preparatory groundwork; excessive delegation; a narrow framework of consent and privacy; risks of exclusion, especially due to dependence on an

[1] NDTV (Aug. 2020). *PM Modi Announces National Digital Health Mission: "Health ID For Each Indian"* [Video]. YouTube. https://www.youtube.com/watch?v=76L__Z28KFo.
[2] Press Trust of India (Aug. 2020). *National Digital Health Mission rolled out on pilot mode in 6 union territories*. Economic Times. Available at: https://health.economictimes.indiatimes.com/news/health-it/national-digital-health-mission-rolled-out-on-pilot-mode-in-6-union-territories/77567210 (accessed on 16/08/2020).
[3] Sharma, Neet Chandra (Dec. 2020). *Centre approves health data management NDHM-HDMP of NDHM*. Livemint. Available at: https://www.livemint.com/news/india/centre-approves-health-data-management-NDHM-HDMP-of-ndhm-11607962291863.html (accessed on 15/12/2020).

Aadhaar-based authentication system; and possibilities of data monetisation by private sector entities.

First, digitisation of an individual's complete health records and linking it with a unique identifier risks confidentiality and privacy of medical data. This can have severe implications for individuals, community and society at large, including stigmatisation, discrimination in employment and insurance, profiling and surveillance. For example, a recent RTI query revealed that the chief medical officer in the Kulgam district of Jammu and Kashmir non consensually shared users' data from the contact tracing app, *Aarogya Setu*, with the local police authorities.[4] These risks necessitate that the NDHM-HDMP be supported by law rooted in the rule of law, and a robust accountability and transparency framework. The Supreme Court of India, in *Justice K. S. Puttaswamy (Retd) Vs Union of India*, held that privacy of medical/health data is a fundamental right under Article 21 of the Constitution. Consequently, any policy with a significant bearing on the right must be governed by law.[5] In view of this, the fact that the NDHM-HDMP is being implemented without a health-specific or general data protection law, may be amenable to a constitutional challenge.

In addition to a law, the task of developing EHRs requires assessment of health system preparedness, building infrastructure capabilities, estimating financial implications, and undertaking pilot studies. While the UHID project has been launched and digital health IDs are being issued in different parts of India, these preliminary steps have either not been concluded or have not yet been undertaken. Hasty implementation without adequate safeguards and preparation not only risks the privacy and security of medical data, it may also undermine general trust in the system leading to low uptake.

Second, many crucial details in the NDHM-HDMP, particularly those related to governance of the UHID and EHR project, will be specified at a later stage. The composition and functioning of the regulator, the procedure for grievance redress, and the processes for de-identification and anonymisation, are cases in point. Such delegation of legislative powers, especially in the absence of a law laying down the overarching legislative policy and guiding principles, is problematic and may run afoul of the Indian Constitution.[6]

Third, there are concerns about the consent and privacy framework. The complete absence of any consent requirement for the creation of UHID, as well as strict access

---

[4] Bhatnargar, Gaurav Vivek (Apr. 2021). *Aarogya Setu Data Was Made Available to J&K Police in Kulgam, Reveals RTI*. The Wire. Available at: https://thewire.in/government/aarogya-setu-data-was-made-available-to-jk-police-in-kulgam-reveals-rti (accessed on 05/04/2021).

[5] (2017) 10 SCC 1. Also see, State of M.P. v Bharat A. 1967 SC 1170.

[6] See, *Agriculture Market Committee vs Shalimar Chemical Works Ltd.* (1997) 5 SCC 516; *Ajoy Kumar Banerjee vs Union of India*. (1984) 3 SCC 127; *In re: Delhi Laws Act.* AIR 1951 SC 332.

control to regulate who can access personal data and to what extent, are some of the chief concerns. For example, media reports point to the use of the Co-WIN portal to surreptitiously create digital health IDs for individuals without their knowledge or consent.[7] Apart from these concerns, there is ample scope to strengthen the framework to empower data principals, through information sheets, in-person counselling and digital literacy programmes.

Fourth, reliance on an Aadhaar-based verification system may lead to large scale exclusion from healthcare services. During the COVID-19 pandemic, there have been multiple instances of the compulsory use of Aadhaar for accessing public health services, which have resulted in many citizens being unable to avail key medical services and get vaccinated.[8] Such situations must be avoided under the UHID and EHRs project.

Fifth, allowing private commercial entities, such as insurance and pharmaceutical companies, to access health data for research, statistical analysis or developing diagnostic tools, entails its own risks such as health data monetisation. The risks are exacerbated in the face of unclear systems for anonymisation and de-identification, as well as absence of strict access control requirements. These issues will not only add another concern to privacy and data security, but also impact a range of legal-ethical issues, rights and public interest, such as discrimination in employment and insurance settings.

At the heart of the NDHM-HDMP is the fundamental right to privacy; for it to be breached a much higher justification is essential. It is far from clear that the NDHM-HDMP, with all its gaps, meets that standard. In this background, it is imperative that the identified shortcomings are addressed prior to implementing the NDHM-HDMP and making the shift towards digital health records, so as to meet the goals of the NDHM.

---

[7] Dogra, Sarthak (May, 2021). *Took Covid vaccine using Aadhaar? Your National Health ID has been created without your permission*. India Today. Available at: https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24 (accessed on 24 May 2021).

[8] For example, the Gurugram Administration imposed a rule that an Aadhaar card with a Gurugram address was mandatory for getting a COVID-19 bed at hospitals. Similarly, several states mandated Aadhaar cards for conducting RT-PCR tests. See, Pati, Ipsita (Apr. 2021), *Aadhaar rule for hospital beds leaves many stumped*. Times of India. Available at: https://timesofindia.indiatimes.com/city/gurgaon/aadhaar-rule-for-hospital-beds-leaves-many-stumped/articleshow/82188572.cms (accessed on 8th June, 2021); Kharb, Sudhir Kumar (Aug. 2020). *'Due to Ambiguity Over Valid ID Proof, I Was Denied COVID-19 Test'*. The Quint. Available at: https://www.thequint.com/my-report/denied-covid-19-test-due-to-aadhaar-id-proof#read-more (accessed on 20 September 2020).

.

The rest of the article is organised as follows: section 2 provides a brief history of the events leading upto the NDHM-HDMP; section 3 discusses important prerequisites for establishing a digital health records system; sections 4-8 analyse the NDHM-HDMP; and section 9 concludes.

2 Background

Information Communication Technology (ICT) based health information systems (HISs) are expected to transform the efficiency and quality of healthcare provision, and are seen as key enablers for achieving Universal Health Coverage (UHC). The use of ICT in health was first endorsed by the World Health Assembly in 2005.[9] In 2006, the Indian government launched the National e-Governance Plan (NeGP), seeking to promote e-Governance initiatives across the country.[10] Around the same time, various public HISs were being set up under different national health programmes. The Integrated Disease Surveillance Programme (IDSP), District Health Information System (DHIS2), National Health Mission Health Management Information System (NHM-HMIS), Mother and Child Tracking System (MCTS) and NIKSHAY are some examples.[11] In 2011, the NeGP apex committee approved 'health' as one of its mission mode projects.

While the various public HISs developed and functioned in silos, the *National Health Policy 2017* (NHP) envisaged the creation of a digital health technology ecosystem, including an integrated national health information system, which "serves the needs of all stakeholders and improves efficiency, transparency and citizens' experience."[12] In 2018, the Ministry of Health and Family Welfare released a draft *Digital Information Security in Healthcare Act* (DISHA) Bill, providing for the establishment of a National Digital Health Authority and HISs across the country.[13] Alongside, Niti Ayog proposed the idea of a National Health Stack (NHS), a shared digital infrastructure to facilitate collection of comprehensive healthcare data with linkages across public and private healthcare. Key components of the NHS included creation of national health registries,

[9] World Health Assembly, 58 (2005). *Resolution 58.28: eHealth.* World Health Organisation. Available at: https://apps.who.int/iris/bitstream/handle/10665/20378/WHA58_28-en.pdf;jsessionid=B7F1B7BCFA0BE7698F5C29D5D77FFCAF?sequence=1 (accessed on 09/02/2021).

[10] For more information on NeGP, see Ministry of Electronics and Information Technology, *National e-Governance Plan*, available at: https://www.meity.gov.in/divisions/national-e-governance-plan (accessed on 01/03/2021).

[11] For an evaluation of various government HISs, see Faujdar et. al. (2019). *Public health information systems for primary health care in India: A situational analysis study*. J Family Med Prim Care 8(11), pp. 3640-3646.

[12] See, Clause 23, Government of India (2017). *National Health Policy 2017*. Ministry of Health and Family Welfare, Government of India (p. 25).

[13] Government of India (2018). *Placing the draft of "Digital Information Security in Healthcare Act (DISHA)" in public domain for comments/views-reg*. F. No. Z-18015/23/2017-eGov. Ministry of Health and Family Welfare (eHealth Section). Available at: https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf (accessed on 20 September 2020).

digital health ID, personal health records framework and a national health analytics framework.[14]

These initial efforts culminated in the National Digital Health Blueprint (NDHB) in 2019. The NDHB provides the layout for developing a digital health ecosystem, delivering a variety of digital health services such as telemedicine, real-time public health surveillance, implementing *Ayushman Bharat* and other government health programmes, hospital management systems, facilitating insurance claims, and creating multiple access points to healthcare and wellness related services. The NDHB proposes a specialised agency called the NDHM, for developing and monitoring the ecosystem.[15] This entails collecting and storing health data at different levels; and facilitating real-time exchange of health data. Some core responsibilities of the NDHM include establishing a digital health ID or UHID, National Health Electronic Registries, a federated EHR Framework and a National Health Analytics Platform.[16] In 2020, the COVID-19 pandemic further catalysed the move towards a digital health technology ecosystem in Indian healthcare.

In this context, on 15 August 2020, the Prime Minister of India launched the NDHM.[17] Subsequently, the Indian government announced the rollout of digital health IDs in six union territories on a pilot basis, and approved the NDHM-HDMP.[18] The main objective of the NDHM-HDMP is statedly, "to create a system of EHRs which is easily accessible to individuals and health service providers and is purely voluntary in nature, based on the consent of individuals, and in compliance with international standards and/or other relevant standards related to data interoperability and data sharing as may be notified for the implementation of NDHM from time to time."[19] The NHDM-HDMP provides for the creation of digital Health IDs for individuals, health professionals and health facilities; and the collection, consolidation, maintenance and sharing of personal and aggregated health data.

In the subsequent sections, we analyse some key components of the NDHM-HDMP, including the governance structure, consent management framework, data security and privacy, risks of exclusion of different population groups, and the implications of private sector involvement.

---

[14] Niti Ayog (2018). *National Health Stack: Strategy and Approach*. Government of India (pp. 18-33).
[15] See, Government of India (2019). *Institutional Framework*, in: National Digital Health Blueprint. Ministry of Health and Family Welfare, Government of India (pp. 39-48).
[16] Ibid, p. 40.
[17] Supra, note 1.
[18] Financial Express Online (Aug. 2020). *Health ID pilot programme to start with 6 Union Territories*. Financial Express. Available at: https://www.financialexpress.com/lifestyle/health/health-id-pilot-programme-to-start-with-6-union-territories/2056613/ (accessed on 13 September 2020).
[19] See Clause 3, *National Digital Health Mission: Health Data Management Policy, 2020*.

3 Prerequisites to a digital health records system

Before delving into specific components of the NDHM-HDMP, we discuss two important prerequisites for a digital health records system: (a) a robust legal foundation underpinning the system, that protects against loss of privacy and security of individual data; and, (b) a thorough evaluation of health system preparedness and government capacity to implement the system.

3.1 Legal foundation

The NDHM-HDMP seeks to digitise health records and link these records with a digital health ID, entailing significant risks to confidentiality and privacy. A study on identity management systems in Europe describes UHIDs as 'one of the most privacy-invasive tools of eHealth', especially because of the potential of linking health data with other data sources.[20] For example, the use of Aadhaar to create a UHID can be linked with other personal information, creating a bearing surface for state surveillance and profiling for commercial purposes. A recent RTI query revealed that the chief medical officer of the Kulgam district in Jammu and Kashmir, was sharing *Aarogya Setu* users' data (without the users' knowledge and consent), with local police authorities.[21] Apart from this, identity fraud, data theft and reidentification are some other risks posed by a digital health ID.[22] In January 2021, a technology portal reported leaking of COVID-19 test results and personal information of thousands of patients, from the websites of multiple Indian government departments.[23] Such breaches can cause embarrassment, humiliation, loss of reputation and stigmatization of individuals, especially vulnerable populations; and unregulated access by third parties can lead to discrimination against individuals, such as denial of insurance and discrimination at workplace.

While it is not possible to entirely eliminate the possibility of harm, a strong legal foundation, rooted in principles of proportionality, accountability and transparency, can mitigate the possibility of harm. The Supreme Court of India, in *Justice K. S. Puttaswamy (Retd) Vs Union of India*, held that confidentiality and privacy of

[20] Els, S. and Mark, L. (Eds.). (2008). *D4. 11: eHealth identity management in several types of welfare states in Europe*. Future of Identity in the Information Society. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.522.6177&rep=rep1&type=pdf (accessed on 20 September 2020).
[21] Supra, note 4.
[22] UNAIDS (2014). *Considerations and Guidance for Countries Adopting National Health Identifiers*. UNAIDS Information Production Unit (pp. 40-41). Available at: https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf (accessed on 20 September 2020).
[23] Sharma, Ax (Jan., 2021). *Indian government sites leaking patient COVID-19 test results*. Bleeping Computer. Available at: https://www.bleepingcomputer.com/news/security/indian-government-sites-leaking-patient-covid-19-test-results/ (accessed on 15 January 2021).

medical/health data is a fundamental right under Article 21 of the Indian Constitution.[24] Consequently, any policy with a significant bearing on this right must meet the four tests laid by *Puttaswamy*, i.e. the measure must be (a) a *procedure established by law* aimed at a *legitimate goal*; (b) *just, fair* and *reasonable*; (c) *proportionate* to the objective sought to be achieved; and (d) have *procedural guarantees to check against abuse* by state or non-state actors.

The need for strong data protection laws to implement digital health is recognised and emphasised globally. As far back as 2006, the World Health Organisation recommended governments, as a prerequisite to digitisation efforts, to enact a comprehensive data protection law and build capacities to regulate all processes related to data, protect rights to consent, confidentiality and privacy, and safeguard individual health data from unauthorized access, abuse and theft.[25] In 2017, The *Puttaswamy* judgment called for the enactment of a comprehensive data protection law in India, codifying globally established privacy and data protection standards and rights of data subjects.[26] In 2018, the World Health Assembly, while recognising the potential of digital technologies to support health systems, called upon member states to develop legislation around issues such as data access, sharing, consent, security, privacy and inclusivity consistent with international human rights obligations.[27]

In contrast to the recommended practise, the UHID and EHRs programme is being rolled out in the absence of any data protection law. Without any statutory foundation and an independent regulatory authority, establishing and implementing a digital health records system; and sharing data with government bodies and private entities across different digital technology products, services and applications, risks fundamental rights to informed consent, confidentiality and privacy. Such an action may be contrary to the Indian Constitution.

3.2 State capacity

Apart from a robust legal foundation, successful implementation of a digital health records system entails health system preparedness, i.e. an assessment of existing capacities for medical record documentation and health information exchange. The WHO recommends governments to do the groundwork on evaluating the state of healthcare documentation for data standardisation and accuracy, technical

[24] Supra, note 5.
[25] World Health Organisation (2006). Electronic Health Records: Manual for Developing Countries. World Health Organisation. Available at: https://apps.who.int/iris/bitstream/handle/10665/207504/9290612177_eng.pdf?sequence=1&isAllowed=y (accessed on 13 September 2020).
[26] Supra, note 5.
[27] World Health Assembly, 71 (2018). *WHA 71.7: Digital Health*. Available at: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf (accessed on 13 September 2020).

infrastructure capabilities, availability of skilled human resources and training for data entry and analysis, protocols for ensuring privacy, security and adequate quality of data, and other environmental issues like electricity and internet speed.[28]

Pushing the implementation of digital health without adequately taking into account and planning for these requirements will cause more harm than any stated benefit of digitization. Some studies, evaluating existing HISs in India, find several deficiencies particularly in relation to the quality of data being recorded. For example, a 2016 study on HIS on maternal and child health care in Haryana, found the quality of data to be sub-optimal with over-reporting in certain indicators and missing data in other indicators.[29] A 2018 study on MCTS in a district in Orissa, identified poor internet connectivity, incomplete data entries, underreporting, discrepant reporting and inefficient monitoring as some of the factors leading to the poor functioning of the MCTS system.[30] Another 2018 study, which examined efforts to build a UHC HIS in a rural clinic and sub centre in a north Indian state, found shortcomings in infrastructure and human resource capabilities.[31] Poor internet connectivity, long power outages and lack of technical support led to delays in recording data, as well as many cases going unrecorded altogether. The Auxiliary Midwife Nurses (ANM), who were primarily responsible for recording data at these facilities, reported a significant increase in workload requiring 60% of their time to be spent on data entry only. In fact, in countries that have implemented EHRs, several studies and surveys reveal that physicians are dissatisfied with EHRs for reasons of burnout and loss of productivity with consequences for quality of care for patients.[32]

In particular, the NDHM is premised on the assumption of widespread internet connectivity throughout the country, as well as general comfort with using the internet. However, these assumptions may not hold true in most parts of the country. According to the recently released survey results from India's official National Sample Survey

---

[28] Supra note 25, pp. 27-33.

[29] Sharma et al (2016). *Quality of Health Management InformationSystem for Maternal & Child Health Care in Haryana State, India*. PLoS ONE 11(2): e0148449, pp. 7-10.

[30] Dehury R.K and S.C. Chatterjee (2018). *Assessment of health management information system for monitoring of maternal health in Jaleswar Block of Balasore District, Odisha, India*. Indian J Public Health, 62, pp. 261-263.

[31] Sahay, S. et al (2018). *Grand challenges of public health: How can health information systems support facing them?* Health Policy and Technology, 7(1), pp. 2-3.

[32] EHRs interfere with face-to-face discussions with patients; require physicians to spend too much time performing clerical work; and, degrade the accuracy of medical records by encouraging template-generated notes. See, Stanford Medicine (2018). *How Doctors Feel About Electronic Health Records: National Physician Poll by the Harris Poll*. Stanford Medicine. Available at: https://med.stanford.edu/ehr/electronic-health-records-poll-results.html (accessed on 1 March 2021); Miliard, Mike (Nov. 2013). *Docs blame EHRs for lost productivity*. Healthcare IT News. Available at: https://www.healthcareitnews.com/news/docs-blame-ehrs-lost-productivity (accessed on 1 March 2021); Miliard, Mike (Oct. 2013). *Docs 'stressed and unhappy' about EHRs*. Healthcare IT News. Available at: https://www.healthcareitnews.com/news/docs-stressed-unhappy-about-ehrs (accessed on 1 March 2021).

Organization (NSSO) (71st Round), the proportion of Indian households in which at least one member had access to the internet was 16.1% in rural areas, 48.7% in urban areas and 26.7% in rural and urban areas combined.[33] Further, the latest National Family Health Survey, covering 22 states and union territories, revealed that over 60% of women in 12 states and union territories have never used the internet.[34] Needless to say, this is far short of the near universal internet access envisaged by the NDHM.

A nationalised HIS also entails coordination with local authorities and widespread stakeholder consultations, particularly to balance between requirements of data standardisation and capturing local peculiarities. In some instances, lack of understanding of local conditions adversely affected the quality of data being recorded. The 2018 study evaluating MCTS in a district in Orissa, found that the details of data requested in tribal areas did not account for the cultural complexity of such areas, ignoring crucial factors such as literacy levels and tribal-specific practices.[35] In 2020, the Punjab government required all pharmacies and medical shops to share data on people buying medications for cold, cough and fever. The objective was to track persons exhibiting COVID-19 symptoms. However, the practise has remained a non-starter because medical shops and pharmacies are reluctant to record and share this information, due to absence of any set protocols and the stigma attached to COVID-19.[36]

The various deficiencies highlighted in existing HISs will likely impact the implementation and success of the UHID and EHRs project as well. It is for this reason that an implementation plan, with a clear understanding of ground realities as well as a plan to mitigate and overcome possible challenges, is essential. The NDHB identified the following steps for implementing UHID: (a) developing infrastructure and technology capabilities for collection and storage of medical data in a standardised manner, to ensure accurate linking of individuals and healthcare providers; (b) specifying technology standards, particularly anonymisation, consent management, health information exchange and health analytics; (c) enacting supporting laws and national governance standards for consent management, data interoperability, privacy and

---

[33] Chandrasekhar, C.P (Jul. 2015). *The Internet in "Digital India"*. The Hindu. Available at: https://www.thehindu.com/opinion/columns/Chandrasekhar/economy-watch-column-by-cp-chandrasekhar-the-internet-in-digital-india/article7446778.ece (accessed on 1 March 2020).

[34] Press Trust of India (Dec. 2020). *Digital literacy remains a concern as most Indian women have never used the internet*. Economic Times. Available at: https://economictimes.indiatimes.com/magazines/panache/digital-literacy-remains-a-concern-as-most-indian-women-have-never-used-the-internet/articleshow/79736857.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (accessed on 31 January 2021).

[35] Supra note 30, p. 261.

[36] Deol, Taran (Apr. 2021). *Pharmacies were supposed to track Punjab's mild Covid cases, but this is why plan failed*. The Print. Available at: https://theprint.in/india/pharmacies-were-supposed-to-track-punjabs-mild-covid-cases-but-this-is-why-plan-failed/632358/ (accessed on 02/04/2021).

security, and patient safety and data quality; (d) identifying a financing model requiring budgetary support from the Government of India, at least in the earlier years; (e) undertaking pilot studies for critical components of the system; and (f) devising a plan for capacity building.[37]

As on 28 January 2021, a total of 700,403 digital health IDs have been created in the six union territories of India.[38] Evidently, the UHID project is already underway. However, there is no clarity on the scope and status of the various implementation steps, as identified in the NDHB. For example, there is no publicly available document on the rollout of digital health IDs as pilot studies. In fact, it appears that many of the steps are yet to be undertaken. This includes enacting supporting laws; developing protocols for standardisation of medical data, processes and systems for anonymisation and consent management, and general governance standards; financial implications and budgetary support for implementation; and identifying areas for capacity building.

A digital health records system has the potential to significantly enhance the effectiveness, efficiency and quality of healthcare. The success of such a system is contingent upon its widespread acceptability and reusability. However, implementing the system at a national level is a complex process, and requires strategic planning and stakeholder engagement. Hasty implementation without adequate safeguards not only risks the privacy and security of medical data, as well as exclusion and inequities; but it may also undermine general trust in the system leading to low uptake.

In the subsequent sections, we discuss key components of the NDHM-HDMP, beginning with the governance framework.

4 Governance framework

The governance framework regulating a digital health records system will need to balance between establishing and maintaining the system in an efficient and cost-effective manner, and ensuring protection and privacy of individual health data. The task is complex and requires the governance architecture to be *well-structured* so as to provide clear separation between legislative (setting standards), executive (enforcing standards) and adjudicatory duties (grievance redress and penalties); *diverse* so as to

[37] See, Government of India (2019). *Federated Architecture & Building Blocks*, and *Institutional Framework*, in: National Digital Health Blueprint. Ministry of Health and Family Welfare, Government of India (pp. 13-29, 39-48).

[38] Information received from the Ministry of Health and Family Welfare (Feb. 2021). *Response to Online RTI Request Registration No. NHATY/R/E/21/00027*. Government of India (available on request).

include expertise from various fields; *independent* from, yet *accountable* to the government; and appointed through a *fair and transparent selection procedure*.[39]

The key features of the governance framework envisaged under the NDHM-HDMP, are enumerated below:[40]

1. The governance structure will be the same as that for the National Digital Health Ecosystem (NDHE), and will be specified by NDHM. The NDHB envisages that the NDHM will facilitate the evolution of NDHE, including establishing and implementing the National Health Electronic Registries and the Electronic Health Records Framework.
2. The NDHB provides that the NDHM will be a government owned body comprising two separate arms: (a) governing council and board of directors responsible for policy formulation and regulation; and (b) CEO and operations team responsible for implementation of the policies. In addition to this, the NDHM-HDMP provides that the governance structure will consist of committees, authorities and officers at different levels. Specifically, it will consist of a data protection officer (NDHM-DPO) and a grievance redressal officer (NDHM-GRO).
3. The Ministry of Health and Family Welfare and the Ministry of Electronics and Information Technology will provide overall guidance.
4. Specific details in relation to the governance structure will be stipulated from time to time.

Although there is some clarity on the structure of NDHM, the NDHM-HDMP is silent on the size, composition, selection process, tenure, powers, functions, terms of removal, financing and the accountability framework governing NDHM. In contrast, the UK and Australian laws clearly lay out these details in respect of NHS-Digital and Australian Digital Health Agency, respectively.[41] The NDHM-HDMP delegates the task of defining these parameters to the NDHM. In effect, the governance structure of NDHM will be laid out by NDHM itself. This may lead to problems associated with excessive delegation, especially lack of transparency and a weak accountability framework.

In particular, due consideration is required in determining the composition of the governing council and the board of directors of the NDHM. As explained earlier, the task of the NDHM is complex and evolving. This entails that the governing council and board of directors (or the policy-making arm) of the NDHM comprise expertise from various

[39] See, OECD (2014). *The Governance of Regulators: OECD Best Practice Principles for Regulatory Policy*. OECD Publishing.
[40] See, Clause 6, *National Digital Health Mission: Health Data Management Policy 2020*; Government of India (2019). *Institutional Framework*, in: National Digital Health Blueprint. Ministry of Health and Family Welfare, Government of India (pp. 39-48).
[41] See, Schedule 18 of the UK *Health and Social Care Act 2012*; and the Australia *Public Governance, Performance and Accountability (Establishment of the Australian Digital Health Agency) Rule 2016*.

fields, such as health care, clinical safety and governance, health informatics, public administration, consumer health advocacy, technology, privacy and cyber security. As an example, Rule 19 of *Public Governance, Performance and Accountability (Establishment of the Australian Digital Health Agency) Rule 2016* lays out the eligibility criteria, providing for a diverse pool of expertise, for appointment to the Australian Digital Health Agency.

The appointment of government officers as the NDHM CEO and NDHM-DPO is not desirable. The two members are responsible for implementing the UHID and EHR system, including the collection, management and sharing of health data. Government officers holding these key positions may expose the NDHM to pressures from the government and compromise its independence. In contrast, the boards of NHS-Digital and Australian Digital Health Agency, while responsible to the parliament, do not have any government representation.[42]

Next, the NDHM-HDMP lays out the grievance redress and enforcement framework. Clause 32 proposes a process through which data principals may redress grievances with data fiduciaries; Clause 33 obligates data fiduciaries to formulate and implement a personal data breach management mechanism; Clause 34 empowers the NDHM-DPO as the principal authority to ensure compliance; and Clause 35 imposes penalties for any breach.

A grievance redress mechanism entails clear processes embedded in the rule of law, through which aggrieved parties can seek redress or challenge regulatory actions. The grievance redress process contained in the NDHM-HDMP falls short on this count. As a first step, a data principal may complain to the internal grievance officer of the data fiduciary. While the internal grievance officer should resolve the complaint within one month, the process for redress has been left to the discretion of the data fiduciary. Where the complaint is not resolved by the internal grievance officer, it may be referred to the NDHM-GRO. Again, the NDHM-HDMP does not provide the procedure for settlement of complaints before the NDHM-GRO or make any provision for appealing the decisions of the NDHM-GRO. In the absence of these procedures, data principals face the risk of arbitrary rejection of complaints. As an example, one of the most common complaints against Indian health insurance companies, who are free to lay down their own procedure for settlement of insurance claims, is the rejection of claims

[42] See, NHS Digital, *NHS Digital Board Members*. Available at: https://digital.nhs.uk/about-nhs-digital/our-organisation/nhs-digital-board/board-members#further-information (accessed on 29/09/2020); and Australia Digital Health Agency, *Executive Team and Board Members*. Available at: https://www.digitalhealth.gov.au/about-us/executive-team-and-board-members (accessed on 29/09/2020).

without any reasoning.[43] In order to avoid a similar problem, the NDHM-HDMP should lay down the procedure for the receipt and redress of complaints at all levels.

Data fiduciaries are also obligated to formulate and implement a personal data breach management procedure, for monitoring instances of non-compliance or unauthorised use. The provision can be strengthened in two ways. First, awareness about the personal data breach management procedure will empower data fiduciaries to understand, identify and report any breach or non-compliance. Hence, it is not sufficient that the procedure be made publicly available. The data fiduciary should be obligated to disclose all information and any material change to the information on the personal data breach management procedure, directly to the data principal. This information should be presented in a legible and reasonably plain language to the data principal. Second, any instances of breach should not only be notified to NDHM, but also the data principal affected by such breach (For more detailed discussion on this, see section 6).

Finally, the NDHM-HDMP prescribes penalties for non-compliance. These include a ban from participating in the NDHE, and suspension or cancellation of digital IDs of health professionals and health facilities. While the NDHM-HDMP envisages various degrees of possible contraventions, the penalties are limited to a ban, suspension or cancellation of the digital health ID. This may lead to situations where either minor violations go completely unpunished or a large number of penalties are disproportionate to the violation. Both scenarios will undermine implementation of the NDHM-HDMP. Hence, there is a need for rationalisation of the penalty system. The Financial Sector Legislative Reform Commission (FSLRC) proposed a graded system of penalties for violations in the financial sector. The penalties ranged from warnings, corrective actions and monetary penalties to suspension, cancellation and instituting criminal proceedings.[44] The Commission further recommended that penalties should be determined according to the cause of violation, specifically whether the violation was the result of informed intent, serious negligence, mistake or was of a technical nature. In particular, the Commission found the traditional system for the imposition of monetary penalties by specifying the maximum amount of penalty, to be ineffective as deterrence. It recommended that the amount of monetary penalty should be a multiple of the illegitimate gain from the violation.[45] The NDHM-HDMP should incorporate a similar system to ensure that the enforcement mechanism is embedded in the rule of law and in line with the principle of proportionality.

---

[43] Malhotra Et Al (2018). *Fair play in Indian Health Insurance*, Working Paper 18/228, National Institute of Public Finance and NDHM-HDMP (pp. 19-20).
[44] Financial Sector Legislative Reforms Commission (2013). *Report of the Financial Sector Legislative Reforms Commission: Volume I (Analysis and Recommendations)*. Government of India (pp. 35-36).
[45] Ibid, pp. 36-37.

5 Consent and confidentiality

Healthcare is characterised by informational inequality, i.e. the information possessed by a doctor as to the possibilities and consequences of a treatment are much greater than that of the patient, and there is implicit trust in the relationship.[46] One way to address this information inequality and empower patients, is through 'informed consent' in the conduct of doctor-patient relationships. The Supreme Court of India, in *Samira Kohli vs Prabha Manchanda*, held that: "The consent so obtained should be real and valid, which means that the patient should have the capacity and competence to consent; his consent should be voluntary; and his consent should be on the basis of adequate information concerning the nature of the treatment procedure, so that she knows what is consenting to."[47] The same principle has been applied to sharing of medical data as well. The Information Technology Rules 2011 permit the collection and disclosure of personal sensitive data, including medical records and history, only after the written consent of the individual who provides the said data.[48] The 2018 *Puttaswamy* judgement also recognised the salience of user consent with respect to collecting, storing, processing and sharing of any data, including medical data.[49] In 2021, the Karnataka High Court restrained the central government and the National Informatics Centre from sharing *Aarogya Setu* data without the informed consent of users.[50] In addition to informed consent, doctors are also mandated to maintain confidentiality of patient information, diagnosis and treatment. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 prohibits a doctor from disclosing "secrets of the patients that have been learnt in the exercise of his/her profession."[51]

Chapter III of the NDHM-HDMP lays out a consent framework to govern the collecting, storing, processing and sharing of individual health data, with the objective that "Data principals should at all times have control and decision-making power over the manner in which personal data associated with them is collected and processed further."[52] Clauses 9-13 lay out the process for obtaining consent for collecting and processing of

---

[46] Arrow, K. (1963). Uncertainty and the Welfare Economics of Medical Care. *The American Economic Review, 53*(5), 941-973.
[47] AIR 2008 SC 138 (para 32).
[48] See, Rules 3-6, *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*.
[49] See, supra note 5.
[50] Express News Service (Jan. 2021). *Karataka High Court restrains Centre, NIC from sharing Aarogya Setu data.* Indian Express. Available at: https://indianexpress.com/article/india/karataka-high-court-restrains-centre-nic-from-sharing-aarogya-setu-data-7161550/ (accessed on 1 Februrary 2021).
[51] There are three exceptions where a doctor is not bound by secrecy, i.e. (a) on the order of a court of law; (b) where there is a serious and identified risk to the health of a person or community; and (c) in cases of notifiable diseases. See, Regulation 7.14, *Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002*.
[52] See, Clause 8(a), *National Digital Health Mission: Health Data Management Policy 2020*.

data, including in cases of children, mentally ill or incapacitated individuals, and medical emergencies; and clause 14 accords certain rights to data principles in relation to their medical data, including the right to confirmation and access, correction and erasure, restricting or objecting to disclosure, and data portability.

For the purpose of collecting and processing personal data, data fiduciaries are obligated to furnish a privacy notice and obtain the express consent of data principals.[53] The consent must be freely and clearly given; informed as to the scope of the consent; specific as to the purposes of collecting or processing the data; and capable of being withdrawn at any time.[54] In the case of sensitive personal data, the data fiduciary must also inform the data principal of any harms that may be involved in the processing of such data.[55] Finally, the consent may be obtained on a physical paper or electronically, either directly from the data principal or through an electronic consent manager.[56]

The NDHM-HDMP rightly puts the autonomy of the data principal as its guiding principle, in relation to the collection, storage, processing and sharing of medical data. However, certain concerns remain. First, the mandatory requirement of taking informed consent is limited to the collection and processing of personal data, and the same requirement is not explicitly extended to the creation of a UHID.[57] Reportedly, the central government is automatically generating UHID numbers for all individuals who choose to get COVID-19 vaccines by presenting their Aadhaar number, without the consent or knowledge of those individuals.[58] This is at odds with individual autonomy and choice, the guiding principle of the NDHM-HDMP consent framework.

Secondly, the consent is required to be specific only as to the purpose for collecting and processing personal data. In effect, the data fiduciary can secure one-time consent of the data principal for collecting and processing personal data for one or more broad purposes, as identified by the NDHM.[59] This is evident from the fact that the data fiduciary is required to collect fresh consent only in the event of any change in its privacy policy or in relation to any previously unidentified purpose.[60] Such a policy

[53] See, Clauses 9 and 10, *National Digital Health Mission: Health Data Management Policy 2020.*
[54] See, Clause 9.2, *National Digital Health Mission: Health Data Management Policy 2020.*
[55] See, Clause 9.4, *National Digital Health Mission: Health Data Management Policy 2020.*
[56] An electronic consent manager is based on the consent management framework proposed under the report on data empowerment and protection architecture. See, Clause 11, *National Digital Health Mission: Health Data Management Policy 2020*; NITI Aayog (August 2020). *Draft Data Empowerment And Protection Architecture Report.* NITI Aayog. Available at: https://niti.gov.in/sites/default/files/2020-09/DEPA-Book_0.pdf. (Accessed 19th April, 2021).
[57] See, Clauses 9.1 and 10.1, *National Digital Health Mission: Health Data Management Policy 2020.*
[58] See, supra note 7.
[59] For identified purposes, see National Digital Health Mission (2020). *Purposes for Collection and Use of Personal Data.* Notification No. T-21016/271/2020-eHealth/01. Available at: https://ndhm.gov.in/documents/hdmpolicy/notification/PurposeforCollectionandProcession (accessed on 1 April 2021).
[60] See, Clauses 10.1 and 10.2, *National Digital Health Mission: Health Data Management Policy 2020.*

precludes the data principal from giving or refusing consent on specific lines. For example, the data principal will not be able to withhold consent to digitise specific information or even refuse consent to share specific digitised information, such as abortion, substance use/dependence, HIV/STI status, suicide attempt and other mental illnesses. In order to address this, a broad consent in the beginning must be accompanied with specific consent taken at each instance of data processing and sharing. The specific consent must include the entity with whom information is to be shared, the specific purpose for sharing, and the information that is necessary to facilitate the purpose. To facilitate controlled sharing of personal data, the data fiduciary must be required to put in place systems and processes for 'masking' of data.[61]

Thirdly, the NDHM Personal Data Processing Model Consent Form leaves out crucial information.[62] The form must explicitly mention that the collection of data is voluntary and refusal will not entail denial of services or care that one is entitled to or imposition of any additional cost. The exact duration of retention of the data, by data fiduciaries or any third party, must also be specified.

Fourthly, the consent framework can be further bolstered to empower data principals. For example, the broad consent form should be accompanied with an information sheet explaining the rights to confirmation and access, correction and erasure, restricting or objecting to disclosure and data portability, as well as the process for grievance redress, in an easy to understand language. Further, the consent should not be limited to a pre-printed form with blank spaces for limited handwritten entries and signatures, and should ideally be accompanied with online or in-person counselling.[63]

Finally, low digital literacy levels may impede the ability of data principals to exercise consent in an informed and meaningful manner.[64] Unfortunately, existing schemes for digital literacy have witnessed slow progress. For example, the Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) to usher in digital literacy in rural India, was approved in February 2017 and targeted 6 crore rural households (one person per household). As of March 2021, only around 4.54 crore candidates were enrolled and

---

[61] Data masking or controlled access provides a means for patients to control disclosure of select information in EHRs. See, McGuire, A. et al. (2008). *Confidentiality, Privacy, and Security of Genetic and Genomic Test Information in Electronic Health Records: Points to Consider.* Genet Med 10, pp. 495–499.
[62] See, the *National Digital Health Mission: Personal Data Processing Model Consent Form*. Available at: https://ndhm.gov.in/documents/hdmpolicy/consentform (accessed on 1 May 2021).
[63] Ibid.
[64] A 2017-18 NSO survey found that 18.4% of persons aged 15 and above were able to operate a computer, while 22.9% were able to use the internet. See, National Statistical Office (2020). *Household Social Consumption in Education in India, NSS 75th Round*. Available at: http://mospi.nic.in/sites/default/files/publication_reports/Report_585_75th_round_Education_final_1507_0.pdf.

2.71 crore candidates were certified.[65] In 2019, a report of the Parliamentary Standing Committee on Information Technology presented figures from an independent impact assessment of PMGDISHA, which indicated that (a) only 50.53% of the respondents felt that their training had led to an increased confidence in the use of digital technology and a subsequent increase in earning capacity; (b) only 37.63% of the respondents stated that they used digital technologies for daily office/school work; (c) only 30% of the respondents said that they were using the internet to access government services; and (d) only 24.75% of respondents affirmed that they were able to teach digital skills to their family members after attending the program.[66] The Standing Committee emphasised the need to scale up and conduct quality impact assessments of PMGDISHA and other digital literacy programmes.[67] Additionally, many digital literacy programmes in India focus on the usage of computers, even though most of the country accesses the internet through mobile devices.[68] In light of this, we recommend that the NDHM should facilitate and scale up digital literacy programmes in order to address problems associated with widespread digital illiteracy, which may impede the ability of data principals to choose and consent in an informed manner.

6 Data privacy and security

Statedly, data protection and security is an important part of the NDHM. Indeed, the *raison d'etre* of the NDHM-HDMP is the realisation of the guiding principle, 'Security and privacy by design'.[69] Privacy by design entails incorporating seven foundational principles while designing information management systems, i.e. proactive not reactive, and preventative not remedial; privacy as the default; privacy embedded into design; full functionality; end-to-end security; visibility and transparency; and, respect for user

[65] See, Government of India (Mar. 2021). *Unstarred Question no. 3586: Digital Literacy under PMGDISHA*. Lok Sabha Secretariat. Available at: http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=22560&lsno=17 (accessed on 1 June 2021).
[66] See, Standing Committee on Information Technology (2019). *Review of National Digital Literacy Programme (NDLM) - Problems and Challenges.* Fifty-Ninth Report. Lok Sabha Secretariat. Available at: http://164.100.47.193/lsscommittee/Information%20Technology/16_Information_Technology_59.pdf (accessed on 1 June 2021).
[67] Ibid.
[68] Srivastava, Sumeysh (September 2020). *International Literacy Day: Bridging India's Digital Divide*. Bloomberg Quint Opinion. Available at: https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-digital-divide (accessed on 9th June, 2021).
[69] See, Clause 1, *National Digital Health Mission: Health Data Management Policy 2020.*

privacy.[70] It is through the implementation of these principles, the NDHM-HDMP can fully realise the goal of 'security and privacy by design'.

Chapter V of the NDHM-HDMP lays down a framework for realising the stated goal. Under the framework, data fiduciaries are bound by the principles of accountability, transparency, consent driven sharing, purpose limitation, collection, usage and storage limitation, and the adoption of reasonable security practices.[71] For a start, data fiduciaries must publish a 'privacy by design' policy that details the obligations of the data fiduciary, the security and privacy practices it follows, and the technology to be used for the same.[72] Further, data fiduciaries must conduct a data protection impact assessment, maintain reliable records, and submit to data audits.[73] A similar set of obligations is imposed upon health information users, who are required to follow the principle of data minimisation.[74]

The 'privacy by design' principle is a step in the right direction. However, the overarching concern of large scale processing of health data in the absence of a data protection legislation, remains. Without statutory guidelines for ensuring citizen's digital rights and the security of their data, effective data protection would be difficult to enforce. Even the procedures laid down in the NDHM-HDMP do not contain adequate penalties for non-compliance as a deterrent.[75] Additionally, concerns about surveillance that have been raised by some political actors remain unanswered.[76]

The NDHM-HDMP itself may not be advocating for a strong data protection regime. This is evident from a comparison of the draft and final policy, as well the EU General Data Protection Regulation (GDPR) and the final policy. For example, the draft NDHM-HDMP stated that requests for erasure could be completed if the purpose of processing was fulfilled.[77] However, the final version allows processing till the purpose for which data was collected is no longer necessary, providing fiduciaries with the discretion to decide this.[78] Additionally, the NDHM-HDMP allows the blocking or restriction of personal data

---

[70] For a detailed discussion on the seven foundational principles, see Cavoukian (2006). *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices.* International Association of Privacy Professionals. Available at: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf (accessed on April 19th, 2021).
[71] See, Clause 26, *National Digital Health Mission: Health Data Management Policy 2020.*
[72] See Clause 26.3, *National Digital Health Mission: Health Data Management Policy 2020.*
[73] See Clauses 27, *National Digital Health Mission: Health Data Management Policy 2020.*
[74] See Clause 30, *National Digital Health Mission: Health Data Management Policy 2020.*
[75] For a detailed discussion on penalties under NDHM:HDMP, see section 4 of this paper.
[76] Scroll Staff (September 6th, 2020). *New health data policy may be misused for surveillance: Chhattisgarh minister writes to Vardhan.* Scroll.in. Available at: https://scroll.in/latest/972361/new-health-data-policy-may-be-misused-for-surveillance-chhattisgarh-minister-writes-to-vardhan. (Accessed on 19th April, 2020).
[77] See, Clause 14.1(b)(ii), *Draft National Digital Health Mission: Health Data Management Policy 2020.*
[78] See, Clause 14.1(b)(ii), *National Digital Health Mission: Health Data Management Policy 2020.*

in case of impairment of the legitimate interests of either the data principal or the health information provider, whereas the draft NDHM-HDMP only mentioned the data principal.[79,80] This may allow the health information provider to store and/or process the data principal's health data beyond the consented time-period and for longer than is necessary. The approved NDHM-HDMP also imposes a condition on data portability: it allows for prohibitions against portability in case doing so would lead to the revealing of trade secrets.[81] By way of comparison, the right to data portability guaranteed under Article 20 of the GDPR does not impose such restrictions.[82] While Recital 41 of European Directive 95/46/EC states that a user's right to access information "must not adversely affect trade secrets", the GDPR notes that a 'balancing act' must be conducted, and so 'the result of these considerations should not be that all information is refused to the data subject'.[83]

The NDHM-HDMP also does not envisage a strong accountability mechanism to enforce privacy. For example, in case of breach of security, only notifying the NDHM has been mandated, whereas notifying the data principal has not been made compulsory.[84] An established facet of a robust data protection framework is the reporting of any data breaches to the affected principals. The Personal Data and Information Privacy Code, 2019 that was tabled in the Lok Sabha, for example, includes the right to access information about security breaches under the right to access.[85] The carte blanche given for the processing and usage of anonymised personal data as 'non-personal' data ignores several attendant security hazards.[86] For example, several studies have indicated the increased threat of de-anonymisation, through both direct and indirect measures. When the scale of data expropriation by private entities contemplated by the draft report on the governance of non-personal data is considered, such concerns are only exacerbated.[87] This issue can be addressed by mandating access control, in

[79] See, Clause 14.1(b)(ii), *Draft National Digital Health Mission: Health Data Management Policy 2020.*
[80] See, Clause 14.1(b)(ii), *National Digital Health Mission: Health Data Management Policy 2020.*
[81] See, Clause 14.1(d), *National Digital Health Mission: Health Data Management Policy 2020.*
[82] See, Article 20: Right to data portability, *General Data Protection Regulation 2016*. Available at: https://gdpr-info.eu/art-20-gdpr/ (accessed 9th June, 2021).
[83] Malgieri, Gianclaudio (May, 2016). *Trade Secrets v Personal Data: A Possible Solution for Balancing Rights*. International Data Privacy Law, Volume 6, Issue 2 (pp. 102–116).
[84] See, Clause 33.2, *National Digital Health Mission: Health Data Management Policy 2020.*
[85] *The Personal Data and Information Privacy Code Bill, 2019.* Introduced in Lok Sabha on July 26th, 2019 by MP Dr. D. Ravikumar. Available at: https://drive.google.com/file/d/1DReq96e-FLsSoKUvK94_-VCtu2Y1PE97/view (accessed on 1 January 2021).
[86] Internet Freedom Foundation. *Unconstitutional draft report on non-personal data ignores concerns about privacy and data monopolies*. Internet Freedom Foundation. Available at: https://internetfreedom.in/unconstitutional-draft-report-on-non-personal-data-ignores-concerns-about-privacy-and-data-monopolies/ (accessed on 19th April, 2021).
[87] Committee of Experts on Non-Personal Data Governance Framework (December 16th, 2020). *Draft Report by the Committee of Experts on Non-Personal Data Governance Framework: Version 2*. Mygov.in. Available at: https://static.mygov.in/rest/s3fs-public/mygov_160975438978977151.pdf (accessed on April 19th, 2021).

addition to anonymisation. As an example, the National Centre for Disease Informatics and Research imposes strict conditions in order to prevent unauthorised access to data. This includes maintaining a list of authorised individuals with access to the data repository, as well as limiting access to the extent necessary for the fulfillment of a defined purpose or objective.[88] Finally, the fact that there is no consent mechanism provided for anonymising data may also result in overreach.

The policy also provides the NDHM with the discretionary power to specify acceptable purposes for collecting or processing health data, which may further contribute to excessive data collection.[89] Such issues are further aggravated by the lack of adequate transparency and accountability measures that allow data principals the power to directly hold data fiduciaries and processors to account. Again, this can be addressed through strict access control requirements. As has been argued elsewhere, conflating privacy with security may lead to significant problems.[90] Resilient data management systems must have strong access control mechanisms through which: (a) both the regulator and the data processor can log all instances of access requests and approvals; (b) secure authorisation tokens are generated and authenticated for each approval; and, (c) regular cross-verification of access logs between regulators and processors occurs.[91]

Thus, it is imperative that a robust data protection regime undergird the NDHM-HDMP. In case the need for operationalizing a digital health data framework is dire, stringent security provisions that deal with the aforementioned concerns must be made a part of the NDHM-HDMP itself. Finally, only aggregated data should be stored at the cloud level, with individual electronic health records remaining at the facility level.[92]

7 Inclusion

The COVID-19 pandemic has underlined the importance of a robust public health system that ensures both quality and affordability. Increasing access to public health

[88] See, clause 5, *NCDIR Policy on Data Processing and Disclosure 2017*.
[89] See, Clause 9.3, *National Digital Health Mission: Health Data Management Policy 2020.*
[90] Banerjee & Sagar (March, 2021), *What we must consider before digitising India's healthcare.* The Indian Express. Available at: https://indianexpress.com/article/opinion/columns/national-digital-health-mission-harsh-vardhan-healthcare-sector-7218715/ (accessed on 19th April, 2021).
[91] Banerjee & Sharma (July 4th, 2018). *Protecting data privacy: Authorisation and access control*. Ideas for India. Available at: https://www.ideasforindia.in/topics/governance/protecting-data-privacy-authorisation-and-access-control.html (accessed 19th April, 2021).
[92] Sahay & Mukherjee (Jan. 2020). *Where Is All Our Health Data Going?*. Economic and Political Weekly. Vol. 55, No. 1. Available at: https://www.epw.in/journal/2020/1/special-articles/where-all-our-health-data-going.html (accessed on 19 April 2021).

services is now recognised as crucial. To this extent, the NDHM-HDMP does address issues of inclusion: the policy explicitly lays down a regime of non-exclusion, with respect to both the possession of a health ID and Aadhaar-based verification. It mandates that participation in the NDHE shall take place on a voluntary basis, and that no individual can be denied access to any health service for a lack of a Health ID. Additionally, Aadhaar will not be mandatory for registering for a Health ID, while each data principal shall have the right to opt out of the programme at any time and ask for the de-linking and deletion of their data.[93]

However, whether deliberate or not, the potential for both exclusion and coercion based inclusion still exists. India has already faced several issues with Aadhaar based authentication. The efficacy of Aadhaar based registration for schemes has been studied in various contexts. One study in Jharkhand found that Aadhaar based authentication "either did not reduce errors of inclusion or leakage or did so at the cost of increased exclusion error".[94] Another study for Aadhaar based verification in PDS shops found that the system is "rife with technical issues such as incomplete seeding of cardholder information, biometric failure and administrative gaps such as inadequate failure reporting and back-up systems".[95] Yet another study sampling Aadhaar based authentication in diverse settings such as PDS distribution, NREGA work, LPG subsidies, midday meals, and the National Social Assistance Programme found that "Available evidence does not substantiate any significant gains from Aadhaar-integration in welfare programmes.[96] On the contrary, it has inflicted considerable pain. Apart from (supposedly) one-time costs of enrolment and Aadhaar-seeding, people are now faced with higher transaction costs on a monthly basis (in pensions and the PDS for instance), and in a significant minority of cases, also face exclusion and denial. Even when it works, people suffer from considerable indignities".

Indeed, the CEO of UIDAI had noted that in 2018, authentication failure for government services was as high as 12%.[97] For a crucial sector such as health, such errors may end up having significant ramifications for public health outcomes. Such concerns have already been voiced before: for example, with regards to the Mother and Child Tracking

---

[93] See Clauses 16, *National Digital Health Mission: Health Data Management Policy 2020.*
[94] Muralidharan, K. et al (Feb. 2020). *Identity Verification Standards in Welfare Programs: Experimental Evidence from India.* Working Paper No. 26744. National Bureau of Economic Research.
[95] Menon, S. (2017). *Aadhaar-based Biometric Authentication for PDS and Food Security: Observations on Implementation in Jharkhand's Ranchi District*. Indian Journal of Human Development, 11(3), pp. 387–401.
[96] Khera, R. (Feb., 2013). *A 'Cost-Benefit' Analysis of UID*. Economic and Political Weekly. Vol. 48, No. 5, pp. 13–15.
[97] UIDAI (2018). *PPT on Technicality of Aadhaar* [PowerPoint slides]. Google Drive. Available at: https://drive.google.com/file/d/1bCgZmV5zPnYZ6icvbFxQxUvw4v0-dlzH/view (accessed on 19 April 2021).

System launched in 2009, activists have pointed out the threat of the extraction of data becoming a precondition for the delivery of health services..

Furthermore, the inclusion of Aadhaar for authentication may not be legally defensible. While the NDHM-HDMP says use of Aadhaar will be voluntary for creating a UHID, the FAQs on NDHM website specify that it would be mandatory for doctors for creating a digidoctor id. Consider the extract below:[98]

> *"2) Is Aadhaar mandatory to create a DigiDoctor ID? In Phase I, an Aadhaar enabled DigiDoctor ID is necessary to authenticate the doctor and enable them to e-sign documents. Later versions will allow doctors to enroll using other ID Proofs as well."*

Similarly, the FAQ on Health Facility Registry says:

> *"10) What do I need for registering in the Health ID? A user needs to register using his Aadhaar and his/her registered mobile number linked to the Aadhaar. Once registered, he/she will be automatically directed to the HFR module."*[99]

The mandatory use of Aadhaar for creating Digidoctor ID for doctors and Health ID for health facilities is contrary to the Aadhaar Act post the judgement of the Supreme Court in *Puttaswamy*, which states that Aadhaar can only be made mandatory for government benefits and schemes.[100] At the very least, mandatory use of Aadhaar will have to be supported by notification and no such notification has been issued yet.[101] Further, even the voluntary usage of Aadhaar for creating UHID requires a notification under Section 4 of Aadhaar Act. It is not clear if such a notification has been issued.

It is also unclear whether the proposed framework will be able to accommodate user consent in practice. Experts have stated that the registration for the health ID may be similar to Aadhaar based registration, in that it would be "'voluntary' on paper, but made mandatory by certain institutions, both government-owned and private".[102] Multiple media reports have mentioned cases in which the health ID has been made mandatory. In September 2020, a government hospital in Chandigarh received an order stating that

---

[98] National Digital Health Mission. *DigiDoctor FAQ*. Available at: https://ndhm.gov.in/home/digidoctor_faq (accessed on 19 April 2021).
[99] National Digital Health Mission. *Health Facility Registry FAQ*. Available at: https://ndhm.gov.in/home/health_facility_registry_faq (accessed on 19 April 2021).
[100] Supra, note 5.
[101] See, section 7, *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*.
[102] Rakheja, Harshit (Jan 2021). *Aadhaar-Linked Digital Health IDs To Be Piloted In India's Covid Vaccination Drive.* Inc 42. Available at: https://inc42.com/buzz/aadhaar-linked-digital-health-id-pilot-in-indias-covid-vaccine-drive/ (accessed 19th April, 2021).

enrolling for the health ID was mandatory and urged the hospital to register its employees at the earliest.[103] While the NHA later clarified that the order was a "wrong circular", such cases create an atmosphere of confusion that may lead to the denial of services. Similarly, on January 27th, 2021, the Puducherry Directorate of School Education issued a circular directing all schools (public and private) to instruct parents to create Health ID for "all school-going children and their families".[104] More recently, multiple media reports have mentioned that citizens who have enrolled in the COVID-19 vaccination programme have had their Health IDs created without their consent.[105,106] This is done on the basis of the data entered by citizens and is linked to their Aadhaar, despite several clarifications from the government stating that Aadhaar is not mandatory for receiving a vaccine.[107]

Concerns about 'coercion-based inclusion' also persist. Multiple reports have highlighted the effectively coercive nature of Aadhaar, in which citizens are coerced into registering through the Aadhaar framework for the provision of services.[108] This can also take the form of financial compulsions, especially in the context of healthcare, as can be seen in the All India Institute of Medical Sciences (AIIMS). At AIIMS, if a patient provides their Aadhaar ID they can get the registration charges of Rs. 100 waived off. Such patients are then subsequently issued a Health ID. Such a NDHM-HDMP significantly privileges the usage of AADHAAR and thus effectively amounts to financial coercion towards the adoption of the Health ID.

---

[103] Rana, Chahat (Sep. 2020). *Doctors in Chandigarh compelled to register for the voluntary National Health ID*. Caravan Magazine. Available at: https://caravanmagazine.in/health/doctors-in-chandigarh-compelled-to-register-for-the-voluntary-national-health-id (accessed 19th April, 2021).

[104] Mithun, M.K. (Feb. 2021). *Privacy concerns loom as Union govt begins Health ID enrolment in Puducherry*. The News Minute. Available at: https://www.thenewsminute.com/article/privacy-concerns-loom-union-govt-begins-health-id-enrolment-puducherry-142987 (accessed 19 April, 2021).

[105] Mathew, Ashiln (June 5th, 2021); *Modi government issuing national health ID stealthily without informed consent*; The National Herald; Available at: https://www.nationalheraldindia.com/india/modi-government-issuing-national-health-id-stealthily-without-informed-consent (accessed on 9th June, 2021).

[106] Dogra, Sarthak (); *Took Covid vaccine using Aadhaar? Your National Health ID has been created without your permission*; India Today. Available at: https://www.indiatoday.in/technology/features/story/took-covid-vaccine-using-aadhaar-your-national-health-id-has-been-created-without-your-permission-1806470-2021-05-24 (accessed on 9th June, 2021).

[107] HT Correspondent (May, 2021). *Aadhaar not mandatory for Covid-19 treatment and vaccine: Centre*; The Hindustan Times. Available at: https://www.hindustantimes.com/india-news/aadhaar-not-mandatory-for-covid-19-treatment-and-vaccine-centre-101621099624651.html (accessed on 9th June 2021).

[108] Ramanathan, Usha (Sep. 2018). *Is there such a thing as an "Aadhaar card"?.* The Economic Times. Available at: https://economictimes.indiatimes.com/news/politics-and-nation/view-is-there-such-a-thing-as-an-aadhaar-card-the-confusion-remains/articleshow/66010734.cms?from=mdr (accessed April 19th, 2021).

Public health groups have already expressed concerns about citizens being forced to have yet another document being forced upon them for the usage of health services. Thus, the health ID framework must be revisited. Even if the framework is to be retained, Aadhaar-based verification should be removed so as to ensure that issues related to privacy are at the very least partially addressed.

8 Access to health big data by private entities

Clause 29 of the NDHM-HDMP talks about sharing of de-identified or anonymised data by data fiduciaries. Clause 29.1 states that **"**Data fiduciaries may make anonymised or de-identified data in an aggregated form available as per the procedure set out in Clause 29.5 below for the purpose of facilitating health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions and such other purposes as may be specified by the NDHM."

It is imperative that 'de-identified' and 'anonymized' data should not be conflated. These two processes, although similar in many ways, should not be mistaken for the same thing. Whereas anonymization of data is 'supposed' to be irreversible and not allow for any retracing to the original identifiable information; de-identification does not necessarily mean that an individual cannot be identified from the data set. Hence, the policy must not allow sharing of de-identified data for purposes of research to private entities. Although the recent developments about the possibility of reversing the process of data anonymization raises big questions on the reliability of the process and the privacy that it affords.

The NDHM-HDMP allows data fiduciaries to share health data with entities in the NDHE for purposes of research, which also include insurance and pharmaceutical companies. Research must not use personal health data in individual patient care and the authorization for granting access must not be vested in individual data fiduciaries. This is all the more important as a lot of "research" could actually be data mining for improving marketing strategies, sales and development of products; purposes far removed from the purposes for which individuals trusted providers with their sensitive health data.

Apart from risk to privacy and data security, the use of aggregated health data by private commercial entities have a range of legal and ethical implications, including the potential for market abuse, unfair competition and lack of a level playing field. Digital health records may also be used by private entities to further their own commercial or private interest at the cost of the individuals and public interest. For example:

1. An insurance company may use digital health records to profile and score individuals and offer individualised insurance contracts (as opposed to risk pooling) and premiums that could lead to denial of coverage for high risk individuals and volatility in premium amounts for others depending on their health data. Profiling and individualisation may raise social concerns, in particular if the risk is correlated with low income and low wealth. This would undermine fairness and result in exclusions and discirmianiton against individuals or groups that would need insurance coverage the most.
2. Pharmaceutical companies may use digital health records for targeted marketing to doctors and patients for their products, which may violate regulations on direct drug promotion. In jurisdictions where digitization of health records has been operational for years, the pharmaceutical companies have been using EHRs as marketing tools with the physicians at the point of care. This has a huge impact on patient choice and safety and expenditure on drugs. Infact, some pharmaceutical companies and diagnostic centres may even be forming EHR vendor relationships and even investing in EHR softwares, such as Practise Fusion, to push for their products.[109] Data dredging is another very common occurrence that takes place in the pharmaceutical industry. It involves conducting multiple analyses till one arrives at the result "so hoped for" and the same is reported without truthfully conveying the analytical course undertaken.[110]

Such risks will be exacerbated in the absence of a broad ethics and governance framework, strong privacy and data security standards, risk-based data de-identification and anonymisation processes, and public engagement. Moreover, many consumers lack awareness to identify unscrupulous requests and may give consent to access their personal health data, inadvertently. This entails a higher standard of protection to the data principals. First and foremost, the government should enact a data protection law. A study shows that the General Data Protection Regulation (GDPR) was effective in improving health data protection in Europe.[111]

Specifically, there is scope to strengthen the NDHM-HDMP, especially on protocols for sharing de-identified or anonymised aggregated health data.[112] The NDHM-HDMP

[109] Bulik, Beth Snyder (2015). *Is there a place for pharma in the emerging EHR market?*. Fierce Pharma. Available at: https://www.fiercepharma.com/sales-and-marketing/there-a-place-for-pharma-emerging-ehr-market (accessed on 15 September 2020).
[110] Hirschler, Ben (2018). *Big pharma, big data: why drugmakers want your health records*. Reuters. Available at: https://www.reuters.com/article/us-pharmaceuticals-data-idUSKCN1GD4MM (accessed on 15 September 2020).
[111] Yuan, B., & Li, J. (2019). *The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation*. International journal of Environmental Research and Public Health, *16*(6), 1070.
[112] See, Clause 29, *National Digital Health Mission: Health Data Management NDHM-HDMP 2020*.

should clearly specify that the purposes for sharing health data should be limited to medical and public health research purposes, as well as expressly prohibit sharing of such data for insurance and other commercial purposes.

The DISHA Bill had specifically barred monetisation of health data and sharing of identifiable or anonymised health data with insurance companies (save for settling insurance claims), pharmaceutical companies, employers and human resource consultants.[113] The NDHM-HDMP policy seems to be a big departure on 'big data' from the DISHA Bill, which was placed in the public domain not so long ago.

Some countries also restrict access to de-identified data. For instance, section 16 of the Australian *Health Records Act, 2012* prohibits sharing of de-identified data with insurance companies. The procedure for granting access to aggregated health data should be provided in the NDHM-HDMP. It should include the requirement for obtaining the consent of the data principal prior to sharing, like under section 15 (ma) of the Australian *Health Records Act, 2012*. Finally, the technical processes and anonymisation protocols should be formulated and approved prior to implementation of the NDHM-HDMP.

9 Conclusion

In 2020, the Government of India announced the launch of the NDHM. Soon after, the NDHM-HDMP, a policy to facilitate setting up of a digital health identity and digital health records system, was approved. While the NDHM-HDMP is a step in the right direction, in terms of attempting to incorporate a 'privacy by design' framework, it is reiterated that policy is not law and the NDHM-HDMP is only a patchwork of half-baked measures. In its current form, the NDHM-HDMP cannot ensure that digitization of medical records is undertaken with due protection of individual autonomy, informed consent, confidentiality and privacy. The policy does not establish an independent regulatory authority for the collection, storage, processing and sharing of health data by the government and private sector entities. Further, it simply states that liabilities and penalties will be as per existing law. However, absent a data protection law, the current laws simply don't have adequate penalties to cover different actors and different ways in which data can be breached. In spite of the urgent need to base NDHM in a sound law, the Personal Data Protection Bill 2019 is still pending in the Indian Parliament. Meanwhile, the Indian government is forging ahead with adding more digital health initiatives tied to the NDHM-HDMP framework, including telemedicine and the COVID-19 vaccination drive through the Co-Win portal.

[113] See, Section 29(5), *Digital Information Security in Healthcare Act (DISHA) Bill 2018.*

In these circumstances, scepticism over the hasty implementation of the UHID and EHRs programme is not unwarranted. Apart from an absent legal framework, inadeqaute health system preparedness and lack of an implementation plan, cast doubt on the overall sustainability, scalability and adaptability of the system. The NDHM-HDMP itself contains many loopholes, including excessive delegation of governance and enforcement functions; a constricted digital consent and privacy framework; risk of over reliance on *Aadhaar*-based authentication; and, vague processes for anonymisation and de-identification, as well as absence of strict access control requirements for personal health data.

In the presence of these deficiencies, the UHID and EHRs programme will do little to support the Indian healthcare system in achieving improved health outcomes. In fact, the programme may cause more harm than good, by incurring unnecessary costs, overburdening the already stretched health system, risking the privacy of individuals and excluding vulnerable populations. Hence, it is imperative that the identified shortcomings are addressed prior to the nationwide rollout of the programme. To this extent, active and sustained stakeholder engagement will provide a strong feedback loop to aid in the development of the programme, as well as other components of the NDHM.