The Dialogue™
INFORM ENGAGE IDEATE

April, 2022

Research Paper

INDIA'S DIGITAL HEALTH DREAMS : GETTING IT RIGHT

Authors : Sreyan Chatterjee | Karthik Venkatesh | Eshani Vaidya
Research Assistance : Saksham Malik
Research Intern: Nihal Sahu
Design By: Diksha Kumari

ACKNOWLEDGEMENT

The Dialogue’s research team would like to express its gratitude to all it’s supporters, for their patient guidance, enthusiastic encouragement, and critique which was useful for this report. The team would also like to extend thanks to the participants of the semi-structured interviews for offering their time and resources. We also express our sincere thanks to Mr. Kazim Rizvi, Founding Director of the Dialogue, for his guidance throughout the project.

This study was commissioned by and submitted to Omidyar Network India and has been re-produced with their permission.

All views, analysis, and any errors in this report, unless otherwise cited, are ours. Please reach out at info@thedialogue.co for any requests for correction to this document.

EXECUTIVE SUMMARY

India, with its diversity and density of population, faces myriad issues in the health sector, such as capacity, infrastructure, increased medical debt and decreasing access to healthcare, among others. Healthcare and its associated services are a core function of a welfare state. Governments widely use technology-mediated welfare and service delivery with the implicit objective of improving health outcomes. In India, this GovTech intervention has been envisaged as the Ayushman Bharat Digital Mission (‘ABDM’), which has the broad objective of ‘overseeing the functioning of the digital health data ecosystem’.

A principled approach, which sets out the policy contours for deployment and expansion, coupled with stakeholder involvement at each stage, has the potential to create a system that has crucial utility as public infrastructure. A rigorous analysis of the aims, objectives, and implementation of an integrated digital health system is fundamental, considering healthcare’s central role in a welfare state.

Throughout this Report, we underline technology’s important role in optimising healthcare delivery and management while attempting to manage expectations as to eventual outcomes. We identify gaps in principles involving design, legislation, policy, infrastructure, and operational procedures. The identification of lacunae is aimed at building interventions that harmonise the modular components of the systems, which can bridge the infrastructural shortfall. In writing this Report, our objective is that these interventions and design principles will pave the way for an expansive uptake of the services within the ABDM and, consequently, broader digital health coverage. We hope that this approach will enhance user trust, drive appropriate innovations, and finally, build a model integrated healthcare infrastructure that other countries facing similar resource constraints can replicate.

In Section I, we look at the four pillars on which the digital health ecosystem is built—governance, consent and data sharing, community and cybersecurity—and identify principles and interventions that can make the systems inclusive. It is important that our framework design principles are suitable to the challenge posed by the Indian context. We try to articulate the scope of this challenge by introducing the economic realities of healthcare funding, challenges of geography and population, and underlying problems in public health capacity. We consider the role of digital health as a private-sector industry as well as a public health intervention and consider some common use cases. We also highlight the importance of privacy and security in Electronic Health Records (‘EHR’) systems to build citizen trust.

The report studies the governing structure of the National Health Authority ('NHA') and the ABDM, identifying the legal nature of those institutions and their governance. We call attention to the absence of a legislative framework and suggest that such a framework, characterised by accountability and transparency, with rights and remedies for users, is central to building a citizen-centric ecosystem.

We present a table of framework design principles derived from international use cases, scholarship, and the past learnings of the Indian health system. The table is focused on four broad themes, i.e., user-centric design, privacy standards, security safeguards, and governance. The report recognises the larger mission of ABDM, which include the intended outcomes of providing universal coverage, as well as of creating interoperable, inclusive, and accessible digital highways for service delivery. At this juncture, we highlight the importance of a robust and secure data protection regime with responsive feedback mechanisms backed by transparent and accountable governance structures.

Section II provides an assessment framework that is a useful tool for those assessing the digital health ecosystem. We present an evaluative framework that assesses policy requirements derived from legislation, policy, and best practices in the form of a list of model questions. We then answer those questions in the context of India's ecosystem, characterised by the National Health Stack and the ABDM. The assessment framework is an attempt to capture the flux of law and policy in digital healthcare. We assess policy requirements at the level of legislation, policy, and the implementation of operational best practices. We suggest a model list of questions that may be used to assess a government digital healthcare system, a policy framework, or a digital healthcare provider.

KEY FINDINGS

1. A digital health ecosystem must have a **legal mandate** that lays down governance structures and key principles.

2. In order to create a truly participative and open process, it is important to **include all stakeholders within decision-making structures**, including end-users.

3. A key aspect of developing a transparent and accountable ecosystem is to **establish oversight mechanisms, including social audit frameworks**.

4. In the absence of **standardised policy guidelines**, it is likely that the ecosystem will not have interoperable data sharing practices, which may compromise user privacy.

5. All policy guidelines regarding **cybersecurity must develop a holistic approach** that also focuses on preventative measures, resilience training and victim support.

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

ABDM	Ayushman Bharat Digital Mission
AIDS	Acquired Immunodeficiency Syndrome
AT	Audit Trails
ASHA	Accredited Social Health Activist
EHR	Electronic Health Record
EMR	Electronic Medical Record ("will provide a comprehensive digital view of a patient's medical and treatment history from a single-health facility") [Bajpai & Wadhwa, India's National Digital Health-Mission, ICT India Working Paper, Oct. 2020]
HID	Health ID
HIPAA	The Health Insurance Portability and Accountability
HIS	Health Information System
MoHFW	Ministry of Health and Family Welfare
NACO	National AIDS Control Organisation Act, 1996
NDHB	National Digital Health Blueprint
NHP	National Health Policy (usually refers to the NHP released in 2017 by the Ministry of Health)
NHS	National Health Service, United Kingdom
PDP Bill	Draft Personal Data Protection Bill, 2019
PPP	Public-Private Partnership
SoP	Standard Operating Procedure
UHID	Universal Health ID
UIDAI	Unique Identification Authority of India
WHO	World Health Organization

INTRODUCTION

On September 27, 2021, the Prime Minister of India launched the Ayushman Bharat Digital Mission ('ABDM'), previously known as the 'National Digital Health Mission'. The ABDM's stated objectives include 'strengthening the accessibility and equity of health services' as part of a citizen-centric approach.[1] India's digital health ecosystem aims at using digital interventions to improve service delivery and develop a principle-based system of healthcare.

A principle-based approach, which sets out the policy contours for deployment of this Mission and its expansion, coupled with stakeholder involvement at each stage, has the potential to create a system that has crucial utility as public infrastructure. These principles include accountable governance structures, robust privacy and data protection norms, effective cybersecurity standards, and a community-driven approach towards developing an inclusive healthcare ecosystem. These principles must not be considered in isolation. Instead, they must be included in the discourse around the system design before any roll-out at scale. With the increase in smartphone penetration rates[2] and the growth in the percentage of digital literacy[3] in India, India's former Health Secretary, Sujatha Rao, pointed out that an initiative as transformative as the ABDM must be rolled-out with an achievable timeline within the next two decades or so.[4]

An important aspect of a digital health ecosystem is the enactment of an enabling legislation. It determines the policy contours within which stakeholders are permitted to function and also dictates the synergy and communication networks between these stakeholders. Any initiative with a transformative capacity such as the ABDM, must be careful so as to not allow infrastructure or implementation details to act as regulation, thus displacing duly consulted-upon law.[5]

In the absence of an overarching legislative mandate or a data protection law, the ecosystem must be cognisant of the changes in privacy regulation, policies regarding primary healthcare and ultimately, people's expectations of their data. Democratic governments usually operate on a dynamic 'social license'[6] based on which they must address citizens' concerns. Citizens' perception of this ecosystem, and by extension the State, will be dictated by their actual

[1] Ayushman Bharat Digital Mission, https://abdm.gov.in/ (last visited Nov. 1, 2021)

[2] McKinsey Global, Digital India: Technology to transform a connected nation (2019) , https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.pdf.

[3] National Statistical Office, Household Social Consumption on Education in India (2017-18), (2020).

[4] K. Sujatha Rao, On Digital Health ID, proceed with caution (The Indian Express, Oct. 7, 2021), https://indianexpress.com/article/opinion/columns/digital-health-id-electronic-medical-records-7554392/.Bertalan Meskó et al., Digital health is a cultural transformation of traditional healthcare, 3(38) mHealth (2017), https://doi.org/10.21037/mhealth.2017.08.07.

[5] *See* Benedict Kingsbury, *Infrastructure and InfraReg: on rousing the international law 'Wizards of Is'*, 8 Cambridge International Law Journal 171-186 (2019).

[6] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research*, 11 Asian Bioethics Review 315 (2019), https://link.springer.com/article/10.1007/s41649-019-00100-7

access to entitlements and services.[7] Community engagement with a use-case analysis will create a more participatory health ecosystem. This will, in turn, have a significant impact on the rates of adoption of initiatives like the Universal Health ID ('UHID') or the Electronic Health Records.

A use-case analysis must also include under its ambit the varied expectations of performance of health-related data by other stakeholders in the ecosystem, such as healthcare providers, service providers, regulatory bodies, among others. Our research methodology, therefore, was to provide for framework principles developed from first principles, a set of international and domestic case studies and learnings derived from semistructured interviews. This report underlines the key role that technology plays in optimising healthcare delivery and management. Our research highlights interventions that can encourage collective adoption of the various building blocks of the ABDM, such as the UHID or the Electronic Health Registries.

[7] Silvia Masiero, *Explaining trust in large biometric infrastructures: A critical realist case study of India's Aadhaar project*, 84 EJISDC (2018), https://doi.org/10.1002/isd2.12053.

I. THE WAY FORWARD

A. GOVERNANCE

i. Defining a Mandate

In Puttaswamy I ('the Privacy Judgement'), while outlining the contours of the fundamental right to privacy, the Supreme Court also added:

> *"[T]he state may assert a legitimate interest in analysing data borne from hospital records to understand and deal with a public health epidemic such as malaria or dengue to obviate a serious impact on the population. If the State preserves the anonymity of the individual it could legitimately assert a valid state interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it".*[8]

The Court also noted that digital platforms are a "vital tool of ensuring good governance"[9] and pointed to information technology being a powerful enabler in the "spread of innovation and knowledge if legitimately deployed."[10]

Various strands of legislation such as data protection, insurance and consumer protection laws govern the healthcare ecosystem. The plethora of legislation introduce a degree of ambiguity within this ecosystem, which makes standardising practices a challenge. This ambiguity may also hinder the working of a grievance redressal framework within this ecosystem. The danger of such an ecosystem is that infrastructure may influence future legislation, rather than legislation providing for a strict structure within which stakeholders are permitted to function.[11]

Legislation with built-in accountability and transparency measures would ensure that the wide powers ascribed to the National Health Authority ('NHA') are subject to sufficient checks and balances. However, an accountability framework that is restricted to responsiveness, evaluation and answerability does not have the same effect as one that has a legal mandate to explain and provide remedies. Remedies and participation are essential elements of effective accountability practices.[12]

[8] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Plurality, para 181).

[9] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Plurality, para 181).

[10] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Plurality, para 181).

[11] Benedict Kingsbury, *Infrastructure and InfraReg: on rousing the international law 'Wizards of Is'*, 8 Cambridge International Law Journal 171-186 (2019).

[12] Walter Flores, Community Monitoring for Accountability in Health: Review of Literature, Open Society Foundations(2011), https://www.copasah.net/uploads/1/2/6/4/12642634/literature_review_community_monitoring_social_accountability _in_health.pdf.

In the absence of a defined mandate backing the digital health ecosystem, it is important to provide for the following:

Standardisation	Express Mandate	Consultations
1. A code of ethics must be formulated by a formal governance body.[13] 2. Develop frameworks for data collection, sharing and usage.[14] 3. Develop standards that are in line with other relevant frameworks, such as PDP, NPD, and other evolving legislations. 4. Define appropriate penalties in case of any arbitrary action.[15]	In the absence of a legislation, the following must be expressly laid down: 1. Data protection and cybersecurity principles; 2. Grievance redressal mechanisms; 3. Oversight mechanisms; and 4. Accountability and transparency checks on regulator funding, utilisations, and actions beyond data use.	1. Interventions should only be drafted following a consultative process with all the relevant stakeholders in an open and transparent manner. 2. Such engagement must be regular and periodic (for example, annual or monthly meetings as appropriate).

ii. Private-Public Interface

The ABDM clearly establishes its commitment towards interoperability, open APIs, a sandbox, and other means that enable private innovation. For example, the UHI consultation paper draws attention repeatedly to the role of private parties in the ecosystem, both as stakeholders and as developers of end-user facing applications, such as consent managers, e-health applications, private locker applications, and others.[16]

Some models of public-private interfaces have worked in the past. Learnings from those projects, which have been effective in the healthcare sector, can be migrated here. For example, under the National AIDS Control Organisation (‘NACO’) the Integrated Counselling and Testing Centres (‘ICTC’) were established in large maternity homes and missionary and charitable hospitals as a result of a public-private partnership (‘PPP’).[17] Similarly, the public-private partnership (‘PPP’) approach was adopted to implement the National Dialysis Services Programme in district hospitals.[18]

[13] FICCI, Leapfrogging to a Digital Healthcare System: Re-imagining Healthcare for Every Indian (2020), https://ficci.in/spdocument/23337/FICCI-BCG-HEAL-2020-Report.pdf

[14] FICCI, Leapfrogging to a Digital Healthcare System: Re-imagining Healthcare for Every Indian (2020), https://ficci.in/spdocument/23337/FICCI-BCG-HEAL-2020-Report.pdf.

[15] FICCI, Leapfrogging to a Digital Healthcare System: Re-imagining Healthcare for Every Indian (2020), https://ficci.in/spdocument/23337/FICCI-BCG-HEAL-2020-Report.pdf

[16] UHI Consultation Paper, p. 11

[17] Sujatha Rao, Do We Care? 232 (2016).

[18] Sujatha Rao, Do We Care? 389 (2016).

In order to be successfully operationalised, a PPP initiative must have the following elements :

Governance Mechanisms	Community Engagement and Transparency
1. Provide institutional mechanisms for: a. Monitoring compliance with contracts; b. Oversight mechanisms; and c. Safeguards to penalise fraud.[19] 2. Evolve standard operating procedure (‘SOPs’) for onboarding private entities and publish information of those onboarding from time to time. 3. Provide clearly defined contractual obligations that are open to public scrutiny.[20] 4. Develop and enforce reporting obligations to monitor progress, identify shortcomings and develop an action plan.	1. Provide citizens with information regarding data usage, expected benefits, harm-minimisation strategies, degree of security and encryption research results, among others.[21] 2. Analyse benefits, costs, fiscal implications, and-long-term impact of every collaboration.[22] 3. Conduct stakeholder engagement proportional to the scale of the PPP to determine: a. Expectations of data usage; and b. Limitations of use.[23]

iii. Oversight Mechanisms

Institutional oversight mechanisms play a significant role in ensuring the smooth functioning and overall success of a public-private partnership. The NITI Aayog has a PPP vertical that is the ‘preferred mode for the implementation of infrastructure projects.[24] The vertical conducted appraisals of 125 PPP projects from 1 April 2020 to 31 March 2021.[25] One of the initiatives under the health sector is a scheme for inviting private investment in medical education.[26]

As a former Union Secretary at the Ministry of Health and Family Welfare has pointed out, the key pillars of a successful PPP initiative in India are that of transparency,[27]community engagement[28] and institutionalised checks and balances.[29]

[19] Sujatha Rao, Do We Care? 84 (2016).

[20] Sujatha Rao, Do We Care? 84 (2016).

[21] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315 (2019).

[22] Sujatha Rao, Do We Care? 419 (2016).

[23] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315 (2019).

[24] Public-Private Partnerships (NITI Aayog), https://www.niti.gov.in/verticals/ppp (last visited Nov. 2, 2021).=

[25] Public-Private Partnerships (NITI Aayog), https://www.niti.gov.in/verticals/ppp (last visited Nov. 2, 2021).=

[26] Annual Report 2020-2021 (NITI Aayog), https://www.niti.gov.in/sites/default/files/2021-02/Annual-Report2020-2021-English_0.pdf.

[27] Sujatha Rao, Do We Care? 84 (2016). Angela Ballantyne & Cameron Stewart, B*ig Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315, 326 (2019).

[28] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315, 326 (2019).

[29] Sujatha Rao, Do We Care? 84 (2016).

Most PPP initiatives, at least within the healthcare sector, are operationalised at the district level stage.[30] They do not have the capacity to undertake measures that provide a sufficient check against arbitrary action, fraud or quality markers.[31] The Government, therefore, plays an important role in delineating roles within the collaboration, providing sufficient checks and balances and providing citizens with transparent processes.[32]

An oversight mechanism established by a regulator will not only monitor compliance against the standardised regulations mentioned in the previous principle but can also enforce penalties for non-performance of contract or violation of regulations. Most countries choose to adopt an independent regulator or institutionalise this committee within their Finance Ministry.[33] Ethical governance of established PPPs, as done under the NITI Aayog, will allow the digital healthcare ecosystem to maximise the potential of Big Data in healthcare and successfully incorporate a consultative, stakeholder-driven approach.[34]

Constitution of Committee	**Responsibilities of the Committee**
1. Monitoring must be done at three levels: a. Monitoring compliance with contracts; b. Oversight mechanisms; and c. Safeguards to penalise fraud. 2. A monitoring committee within the concerned Ministry reviews the progress and approves approval of states. 3. States, through a nodal agency, monitor the project. 4. Local/district level management to run quality assurance, provide data points and assist in audit mechanisms.[35]	1. Recommend social audits as per need.[36] 2. Develop a procedural manual for those within the committee (assign responsibilities and accountability).[37] 3. Publish annual compliance reports with: a. Status of compliance with standardised regulations and contracts;[38] b. A review of the grievances of users and manner and extent of redressal provided;[39] and c. This body could also publish social audit reportsfor projects under PPP.

[30] Sujatha Rao, Do We Care? 84 (2016).

[31] Sujatha Rao, Do We Care? 84 (2016).

[32] The NHS-DeepMind collaboration in the United Kingdom was not well received because citizens were not aware of the nature of data that the private entity had access to. This had a significant impact on the level of trust the citizen held with the state because the citizen will always look to the state to operate within the social license and protect their interests, while private entities do not have the same responsibility. Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315, 326 (2019)

[33] Burger & Hawkesworth, *How to Attain Value for Money: Comparing PPP and Traditional Infrastructure Public Procurement*, 2011/1 OECD Journal on Budgeting 1, 10 (2011).

[34] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315, 326 (2019).

[35] Alex van den Heever, *Developing coordinated public-private partnerships and systems for financing health in Africa: Experiences from Africa and India*, African Dev. Bank (2017).

[36] Planning Commission, Institutional Mechanism for Monitoring of PPP Projects (2012), https://niti.gov.in/planningcommission.gov.in/docs/sectors/ppp_report/reports_guidelines/Guidelines%20for%20Monitoring%20of%20PPP%20Projects.pdf.

[37] Asian Development Bank, Public-Private Partnership Handbook (2008),https://www.adb.org/sites/default/files/institutional-document/31484/public-private-partnership.pdf

[38] Planning Commission, Institutional Mechanism for Monitoring of PPP Projects (2012), https://niti.gov.in/planningcommission.gov.in/docs/sectors/ppp_report/reports_guidelines/Guidelines%20for%20Monitoring%20of %20PPP%20Projects.pdf.; Asian Development Bank, Public-Private Partnership Handbook (2008), https://www.adb.org/sites/default/files/institutional-document/31484/public-private-partnership.pdf.

[39] Planning Commission, Institutional Mechanism for Monitoring of PPP Projects (2012), https://niti.gov.in/planningcommission.gov.in/docs/sectors/ppp_report/reports_guidelines/Guidelines%20for%20Monitoring%20of%20PPP%20Projects.pdf.; Asian Development Bank, Public-Private Partnership Handbook (2008), https://www.adb.org/sites/default/files/institutional-document/31484/public-private-partnership.pdf.

B. CONSENT AND DATA SHARING

i. Consent Managers

Consent managers help route the data flow such that patient consent is recorded, and the subsequent transaction is logged. Consent managers will be the designated intermediaries that will operationalise the consent norms that are laid out either through legislation (PDP Bill 2019) or other relevant policies such as the National Health Data Management Policy. HIE-CM (ABDM Health Records Application), owned by NHA, is currently the default consent manager for ABDM.[40] However, multiple consent managers are likely to be available in the future as a result of open APIs, allowing the end user to choose the service provider appropriate to their needs.[41]

Considering consent managers are key in the ecosystem that allows for data flows, some aspects of their functioning and the life cycle of consent need to be clearly defined. Consent managers must be regulated entities. At present, there is some ambiguity regarding which provisions are applicable for consent managers that if they fall under data processors/fiduciaries is still unclear and is a point of debate in other jurisdictions as well.

Consent Management

1. Users must be informed in case the context of processing data was altered. A fresh consent mechanism must be initiated.
2. Consent managers must undergo checks and must align their corporate governance practices in a manner that benefits the end user.
3. Ensure regulation of consent managers in the health sector through a principle-based framework. Avoid centralized regulation of all consent managers, and instead build sector-specific capacity and expertise.
4. Distinguish between Account Aggregators and Consent Managers in policy documents.

ii. Anonymisation Practices

Health data is sensitive personal data and sharing it requires protections such as pseudonymisation or anonymisation. This would mean that there needs to be a clear indication of the anonymisation standards to be followed for social and healthcare data.[42] Similarly in India, we must evolve these standards for sharing healthcare data. While the report of the Committee of Experts on Non-Personal Data Governance Framework[43] has suggested some possible anonymisation standards, there is no consensus on an optimal solution that can be implemented

[40] ABDM, FAQs, https://abdm.gov.in/home/faq (last visited Nov. 1, 2021)

[41] ABDM Strategy Overview, 2.3.2. ABDM, FAQs, https://abdm.gov.in/FAQ (last visited Nov. 1, 2021)

[42] Digital, ISB1523: Anonymisation Standard for Publishing Health and Social Care Data, https://digital.nhs.uk/dataand-information/information-standards/information-standards-and-data-collections-including-extractions/publications- andnotifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

[43] Ministry of Electronics and Information Technology, Report by the Committee of Experts on Non-Personal Data Governance Framework 48-50 (2020), https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf.

at scale. Having said that, it is crucial to examine how to facilitate data sharing without compromising privacy and minimising risks to the patient.

iii. Data Sharing

The value of data sharing in the healthcare sector, while always known, received greater significance as a result of the COVID-19 pandemic. Data sharing within this ecosystem can improve the effectiveness and quality of treatment (with increased information on co-morbidities, earlier disease intervention and stronger research capabilities); help identify risk factors for disease in a granular fashion, understanding disease transmission pathways and increase of knowledge dissemination (among patients, healthcare providers, researchers etc.)[44] While the benefits of data sharing in healthcare are numerous, the relationship between the state and the citizen is one that warrants examination. The government plays a significant role in the creation of health databases and may be classified as the ‘originators of data’[45] in one sense. It is important, therefore that any and all data sharing practices are conducted for public good and there are smooth and efficient collaborations between the citizens and academia, civil society and other related health entities.[46]

An important aspect of data sharing is that of managing expectations of all the stakeholders involved. In an ecosystem as diverse as healthcare, each stakeholder has a specific set of expectations of data and the outcomes of data-related activities. Healthcare professionals and facilities, for example, collate data to diagnose patients, develop treatment plans, manage symptoms, and encourage patient compliance. Their values of patient data should be shaped by legal, ethical, and medical concerns. Healthcare innovation, however, commonly refers to data and its use in ‘disruptive technology’ that is used to ‘transform institutional arrangements in healthcare.’ The healthcare provider’s value of data, therefore, has patients at the centre, while the value of data, as determined by innovative practices, has consumers at the centre.[47] Therefore, the nature of data collected, nature of use and expectations of eventual outcomes must be clearly expressed by every stakeholder to determine the cohesive value of data.

In order to maximise the potential of data sharing in the digital healthcare ecosystem, it is important to include the following:

[44] European Commission, Study on Big Data in Public Health, Telemedicine and Healthcare (2016), https://ec.europa.eu/health/sites/default/files/ehealth/docs/bigdata_report_en.pdf.

[45] Sridharan et al., Health Data Stewardship: Top-Down State Action for Public Benefit Data Sharing (Aapti Institute 2021).

[46] Sridharan et al., Health Data Stewardship: Top-Down State Action for Public Benefit Data Sharing (Aapti Institute==2021).

[47] Fiore-Silfvast & Neff, *What we talk about when we talk data: Valences and the social performance of multiple metrics in digital health* (EPIC 2013 Proceedings, American Anthropological Association), https://anthrosource.onlinelibrary.wiley.com/doi/pdfdirect/10.1111/j.1559-8918.2013.00007.x.

Standardisation of processes	Data Sharing Agreements	Developing guidelines/ interventions
1. Standardise data sharing for specific use cases to ensure data quality and to ensure that the integrity of data is maintained. For example, epidemic management would need updated and accurate data to prevent exclusion and ensure accountability. 2. Enforce performance standards for data sharing practices across its various forms. 3. Conduct detailed audits/privacy risk assessment/stress tests before any data is shared. The governing body could: a. Ensure that the relevant application employs the appropriate encryption and data minimisation at its output channels; and b. Ensure that the programme only conducts authorised tasks and does not go beyond the prescribed purpose. 4. Develop data access conditionalities for creating apps on the UHI neworks in line with the graded health data sets. 5. Develop audit trails, designate trusted third parties with whom data can be shared.[48]	1. Contracts that allow for data sharing will need to set out the entire lifecycle of data. a. The services rendered; b. The purpose of collection; c. The manner of use of data; d. The form in which data will be used; and e. Duration of use and consequent deletion/long term plans for data. 2. Specify how such data (i.e., shared data) will be monetised. 3. The agreement must be made public.	1. Digital Health Interventions and guidelines must bear the forms of data sharing in mind: a. Data sharing that is premised on consent i.e., where end-use is visible; and b. Data sharing where enduse is not visible (public benefit/between stakeholders for commercial purposes). 2. Mandate periodic participatory meetings with beneficiaries, endusers in order to review policies and make case-by-case decisions where necessary.

iv. Purposes of Collection

A legal mandate must clearly lay down the purposes for which data can be collected. This is required by established tests under the Puttaswamy I (‘the Privacy Judgement’).[49] Disclosing the purpose of data collection also plays a significant role in building a transparent ecosystem and citizen trust.

The NHS-DeepMind collaboration in the United Kingdom was a collaboration that was severely criticised because the ‘appropriate use’ of data was not defined.[50]

[48] Paul Ohm, *Broken Promises of Privacy: Responding to The Surprising Failure of Anonymization*, 57 UCLA Law Review 1701,= 1771-1772 (2010), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1016&context=hightechevents.

[49] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

[50] Angela Ballantyne & Cameron Stewart, *Big Data and Public-Private Partnerships in Healthcare and Research: The Application of an Ethics Framework for Big Data in Health and Research*, 11 Asian Bioethics Rev. 315, 326 (2019).

Define the Purpose of Collection

1. Define primary and secondary uses of data at the time of consent collection.
2. A separate policy[51] must determine the secondary use of health data for statistical, research, and development purposes.
3. Users must be given an option to consent to such sharing, and consent for such purposes must be granular.[52]
4. Data permits for such sharing and flow for secondary uses must bar sharing for advertising, marketing, and insurance purposes.[53]

C. COMMUNITY

With the evolution of disruptive technology and the resultant increase in vulnerability of citizens, it is important to ensure that every concern and expectation of the citizen is deliberated upon and appropriately addressed. Our desk research identified that in order to build a participatory and efficient digital health ecosystem it is important to involve communities in policy making and formulation. Communities must also be a part of the oversight mechanisms deployed to ensure the digital ecosystem is transparent and accountable in nature. This section explores the manner in which communities can play a significant role in maintaining the integrity of the digital health ecosystem and can increase citizen trust in the ecosystem as a whole.

i. Social Audits

Developed as a mechanism to uphold accountability in government schemes, a social audit evaluates whether the on-the-ground realities are in line with the findings published by the Government. Social audits are most commonly conducted at the local levels of governance such as the Gram Panchayats.[54] The community collects primary data (i.e., data provided by stakeholders) and secondary data (i.e., data provided by the government) in order to publish an 'audit report' that evaluates the impact of the scheme implemented in the concerned area.

In the context of a healthcare system, such a mechanism allows for exceptional focus on health rights, devolution of powers and the decentralisation of decision making. Mobilising communities at the grassroot level will also help spread awareness about the benefits of digitisation of healthcare. The reduced information asymmetry will not only have a positive impact on the rates of adoption but will also improve individual agency.

[51] Government of Finland (Ministry of Social Affairs and Health), Secondary use of health and social data, https://stm.fi/en/secondary-use-of-health-and-social-data

[52] Saks et al., *Granular Patient Control of Personal Health Information: Federal and State Law Considerations*, 58 Jurimetrics 411 (2019). See also The Office of the National Coordinator for Health Information Technology, Enabling Granular Choice for Health Care Delivery and Research Consent (2020).

[53] How NHS Digital makes decisions about data access (NHS Digital, Oct. 25, 2021), https://digital.nhs.uk/services/dataaccess-request-service-dars/how-nhs-digital-makes-decision

[54] Meghalaya Community Participation and Public Services Social Audit Act, 2017

Social Audit Committee	Access to Documents	Reporting Requirements	Financial and Human Resources Support
1. Must have statutory backing.[55] 2. Must be institutionalised within a Ministry of the Central Government.[56] 3. Clearly lay down the constitution of the committee and its powers and functions.[57]	1. In order to conduct an accurate evaluation of the impact of the ABDM, the social audit committee must have access to the following data points from stakeholders:[58] a. Performance indicator(KPIs); b. Budget; c. Infrastructure/ Development details; and d. Timelines.	1. Develop a standardised format for reporting (details to be collected, timelines etc.). 2. Create a web portal where timelines, action plans and trackers and audit reports can be published.[59] 3. Submit an Action Report.[60]	1. Conduct training courses. 2. Employ adequate staff. 3. Adhere to Code of Ethics.[61] 4. Adhere to standards (regarding manner of collecting data, reporting requirements etc.)

ii. Grievance Redressal Framework

Citizens must have effective, accessible, and legible authority to raise grievances with. Development of an efficient and independent grievance redressal mechanism will minimise the scope of arbitrary action and make the system more accessible, thereby increasing citizen trust. The National Health Service (‘NHS’) in the United Kingdom provides for a grievance redressal system that is truly effective due to smooth communication channels and minimal information asymmetry. In order to be successfully operationalised, a grievance redressal mechanism could incorporate the following elements:

[55] For example, National Rural Employment Guarantee Act, 2005 (‘NREGA’) or the Meghalaya Community Participation and Public Services Social Audit Rules, 2019 (‘Meghalaya Social Audit Rules).

[56] Sujatha Rao, Do We Care? 354 (2016).

[57] The social audit unit created under the NREGA consists of a social auditor, resource persons from states/districts/villages, a district programme coordinator, and a programme officer.

[58] Jain & Polman, A Handbook for Trainers on Participatory Local Development (Food and Agriculture Organisation 2003), https://www.fao.org/3/ad346e/ad346e09.

[59] Rule 19, Meghalaya Social Audit Rules, 2019.

[60] Rule 20(12), Meghalaya Social Audit Rules, 2019.

[61] Safar India, Documentation: Pilot Social Audits under Meghalaya Community Participation and Public Service Social Audit Act, 2017, p. 16, https://safar-india.org/documents/PILOT%20SOCIAL%20AUDITS.pdf.

Information Sharing	Redressal Process	Resolution
1. Posters (easy to read and in multiple languages) should be put up in hospitals so that patients are aware of their right to seek redress.[62] 2. The posters, and other IEC channels, should ensure that the grievance redressal hotline number and the URL of the website are prominently published. 3. Provide information regarding the first point of contact (preferably at the community level, such as ASHA workers).	1. Allow for phone-based complaint registration through IVR system as well as call centre. Additionally, both phone-based processes and the website should be accessible in local languages. 2. Aggrieved parties must be presented with a receipt that contains details such as, date of filing of complaint, concerned parties, complaint ID, redressal office, name and contact details of the grievance officer and details (such as a URL/direction to create an account) to check on the ‘status’ of their complaint. 3. Adhere to strict timelines with reasons provided for delay of over 6 months.[63] Provide clear penalties/compensation in case grievance redressal is delayed. 4. Ensure processes for grievance redressal at the local level.[64] The system must collaborate with district and state-level health departments to integrate both online and offline processes smoothly. 5. Provide adequate escalation mechanisms to a judicial or quasi-judicial body with power to direct NHA and other relevant bodies.[65]	1. The aggrieved party must have access to the status ofresolution i.e., action taken. 2. Collection of complaint handling data can be used to identify of areas improvement within healthcare providers.[66]

iii. Local Data Management

Local level governance at the level of information security, digitisation, and development of infrastructure can take place through making the information officers of healthcare centres accountable for infrastructure. Additionally, the NHA can provide an easy path to grievance redressal and reporting in cases where digitisation has not properly taken place. Paper-based

[62] National Health Service, How to complain to the NHS, https://www.nhs.uk/using-the-nhs/about-the-nhs/how-tocomplain-to-the-nhs/.

[63] National Health Service, How to complain to the NHS, https://www.nhs.uk/using-the-nhs/aboutthe-nhs/how-to- complain-to-the-nhs/. 66

[64] See NREGA Operational Guidelines 2013, p. 113, https://nrega.nic.in/Circular_Archive/archive/Operational_guidelines_4thEdition_eng_2013.pdf.

[65] Article 78 of the GDPR provides for the “right to an effective judicial remedy against a supervisory authority”.

[66] National Health Service, how to complain to the NHS, https://www.nhs.uk/using-the-nhs/about-the-nhs/how-tocomplain-to-the-nhs/.
Act, 2017, p. 16, https://safar-india.org/documents/PILOT%20SOCIAL%20AUDITS.pdf.

dose-based reporting tools may be helpful.[67] Requiring health facilities to accurately report the usage of numbered and tagged vials have been shown to be highly effective in reducing vaccine wastage.[68]

With the rise of consent managers and a federated architecture, authorities must ensure that no illegitimate data access takes place at health facilities, or any health-related data fiduciaries. Norway's HIS, for example, maintains two separate logs: a regular access log, and an actualization and emergency access log.[69] Log variables, as well as collected information, must be determined in a systematic manner. Additionally, suspicious characteristics on audit trails can be flagged.[70] Audit trails, including paper audit trails, face the limitation of poor reporting standards that can only be remedied through training. Checklists and paper audits have been highly effective in reducing the error rate in surgery, intensive care, and emergency medicine.[71]

In order to successfully operationalise this practice, it is important that the NHA and the ABDM move towards a culture where key performance metrics and funding incentives at every level include a focus on high reliability. These can be measured through the percentage of the process for which SOPs have been created, the level of training and performance reviews for medical professionals and enabling data staff, etc. This can be done through ongoing engagement with the National Health Systems Resource Centre[72] and building on work they have done in terms of quality assurance, checklists, and integrating them into the ADBM system, as well as mandating them in healthcare-professional-facing client applications.

Paper-based Management

1. Build a system of alternatives to smartphones and rich media with low-consumer-tech solutions like (SMS/Phone with Vernacular Access, Biometric Authentication, and Physical Processes).

2. In cases where smartphone access is not available, use generated QR Codes on physical slips/ identity cards as a paper trail for the use of data systems at health facilities.

3. Create a consent management equivalent of a physical passbook, a document issued where any consent requests granted, and access logs can be viewed by citizens without internet or smartphone access. Make physical copies interoperable with digital systems through QR/Barcode.

4. Allow citizens to use physical copies of the UHID medical records at any time. Move from digital-first to digital-physical interoperability with QR Codes, Reference IDs, and other means of linking.

5. Establish strict SoPs and Protocols for actualisation and emergency access:

[67] Rustagi et al., *The effectiveness of a dose-based reporting tool in reducing vaccine wastage at primary care clinics in Delhi, India: an operational research study*, 17 Human Vaccines & Immunotherapeutics 824 (2020), https://doi.org/10.1080/21645515.2020.1796427.

[68] Rustagi et al., *The effectiveness of a dose-based reporting tool in reducing vaccine wastage at primary care clinics in Delhi, India: an operational research study,* 17 Human Vaccines & Immunotherapeutics 824 (2020), https://doi.org/10.1080/21645515.2020.1796427.

[69] *See* Rostad & Edsberg, *A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs*, 22nd Computer Security Applications Conference 175 (2006), https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.190.4413&rep=rep1&type=pdf.

[70] *See* Correia et al., *Illegitimate HIS access by healthcare professionals: scenarios, use cases, and audit-trail based detection model*, 164 Procedia Computer Science 629 (2019), https://www.sciencedirect.com/science/article/pii/S1877050919322768.

[71] Thomassen et al, *Implementation of checklists in health care; learning from high reliability organisations, 19:53. Scandinavian Journal of Trauma*, Resuscitation and Emergency Medicine (2011), https://dx.doi.org/10.1186%2F1757- 7241-19-53. [60]Rule 20(12), Meghalaya Social Audit Rules, 2019.

[72] National Health Systems Resource Center, http://qi.nhsrcindia.org/.

a. Create strict standards and criteria that delineate the circumstances under which actualization or emergency access is permissible;

b. Ensure the use of actualisation or emergency access creates a trail, both physical and digital. Create authorisation and notification protocols for actualisation and emergency access of patient records; and

c. Establish limitations on actualisation-based access, including time limits and requiring periodic reauthorisation by multiple persons, including a senior healthcare professional and an administrative professional across different departments.

iv. Primacy of Health ID

Mandatory authentication with other foundational identifiers will inevitably lead to exclusions in access to welfare schemes and other healthcare services.[73] Data systems should be based on Health ID both as a foundational and a functional identifier, based on context, without mandatory linkages to foundational identifiers.

Ensuring the primacy of one's health ID will ensure that datasets are separated, minimising the possibility of a centralized view of the user's care contexts. In the absence of UHID having a mandatory foundational identifier, it addresses risks of exclusion, and additional risks involved in linking of independent databases containing personal information.[74]

Ensure Primacy of Health ID

1. Amend any existing legislation that might require other foundational identifiers for certain health schemes and benefits, to prevent linkages across datasets.
2. Ensure data minimisation as a principle for citizen agency and ensure that health data is not linked to other foundational identifiers by design for availing health schemes and prefer UHID.
3. Application for a UHID must also accept a wide-ranging set of documents, such as birth certificate, 10th grade marks card attested by a panchayat, PAN card, voter ID etc. in order to be more inclusive.

v. Information, Education and Communication ('IEC')

The use of IEC activities includes dissemination of information to the general populace through social media, advertisements, helplines, posters etc. Commonly used to increase awareness, the popularity and effectiveness of these mechanisms have also allowed them to be used as tools of behavioural change.[75]

[73] See State of Aadhaar: A People's Perspective vi-viii (2019), https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf?utm_source=download_report&utm_medium= button_dr_2019.

[74] Shruti Trikanad, Governing ID: Use of Digital ID in the Healthcare Sector, Centre for Internet and Society (2020).

[75] National AIDS Control Organisation, National Strategic Plan for HIV/AIDS and STI 2017-2024 (2017), http://naco.gov.in/sites/default/files/Paving%20the%20Way%20for%20an%20AIDS%2015122017.pdf

For example, a higher proportion of people that had viewed the advertisements used in the Voluntary Blood Donation Campaign donated blood[76] and IEC activities have played a significant role in reducing the stigma surrounding HIV-AIDS.[77]

The most crucial element of a successful IEC campaign is that of funding. Without adequate funding such campaigns are forced to compromise on the equipment, innovation, IT software deployed, maintenance and training of professionals.

IEC Mechanisms

1. Create a resource repository for individual building blocks (such as the UHID) that has helpful resources like newsletters, policies/guidelines, multimedia, surveys etc.[78]
2. All websites and health services deployed through apps must be accessible to all:

   a. Incorporate different languages; and

   b. Incorporate features to make it accessible by persons with disabilities, such as larger fonts, screen reader options, increased contrast between the foreground and background etc.
3. The IEC department under the NHA must work with local communities, NGOs and civil society to innovate IEC campaigns and reach a wider audience.

D. CYBERSECURITY

The critical nature of health data and its supply chains has made it highly susceptible to cyberattacks. The healthcare data breaches in the United States rose by 39% from 2019 to 2020.[79] The Information Commissioner’s Office in the United Kingdom reported 3,557 health data breaches (nearly 20% of personal data breaches are health data breaches).[80] A study pointed out that hospitals that had faced data breaches in the last three years suffered a higher mortality rate. Cyberattacks have a significant impact on the day-to-day physical operations of a hospital.[81]

Our desk research identified the following shortcomings in the existing mechanisms of cybersecurity: firstly, there is a significant gap in the availability of data regarding cyber-attacks (the breaches, the impact, the vulnerabilities etc.); secondly, we need to evolve a more holistic approach to cyber security; and lastly, the absence of institutionalised cybersecurity regulation for the health sector. This section attempts to operationalise these principles and build more focus on ex-ante i.e., preventative measures of cybersecurity.

[79] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

[80] Info. Commissioner’s Off., Ann. Rep. & Fin. Statements: FY 2019-20, https://ico.org.uk/media/about-the- ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

[81] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

i. Security Frameworks

Health data, given its value, is particularly susceptible to cyber-attacks. Ex-post interventions are inadequate and do not meet the standards of security. Security frameworks must, therefore, be part of infrastructure and regulation. The cybersecurity frameworks deployed must not focus solely on building infrastructure to protect citizens in the aftermath of a data breach or cyberattack but must focus on healthcare preparedness and resilience measures as well.[82] Notifying ABDM systems and health databases as critical information infrastructure would ensure that basic cybersecurity concerns are partially addressed through government oversight, to the extent that it can be effective. However, the sheer number of systems that would be part of the ABDM's federated architecture would require more effective modes of compliance for protected systems. Given the increasing use of technological solutions as a process for 'end-to-end' governance and service delivery, it is necessary to adapt existing compliance procedures under the Information Technology Act, 2000.

Healthcare as Critical Infrastructure

1. Adopt ex-ante measures to address existing vulnerabilities (lack of resources, trained personnel, and outdated infrastructure through capacity building).
2. Make deliberate advances in user protection (support victims of cyberattacks, adequategrievance redressal mechanisms).
3. Develop a healthcare big data security monitoring and early warning system for breaches.[83]
4. Ensure that users receive a notification in the event of a data breach.
5. An emergency response mechanism should be developed in the event of a data breach.[84]
6. Build capabilities and specific defences against cyber espionage to protect intellectual property.[85]
7. Conduct period risk assessments of the cybersecurity system as whole in order to identify shortcomings and improve security mechanisms.[86]
8. Certification and labelling schemes can be adopted across the ecosystem to increase citizen trust in services.[87]

ii. Institutional Mechanisms

Considering the vulnerability of the healthcare sector, cybersecurity mechanisms must be developed to identify the unique risks associated with collecting significant amounts of sensitive personal data. An important aspect of building the aforementioned security frameworks is that there is a separate institutional mechanism for cybersecurity in the health sector. This will also help standardise practices across the sector.

[82] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

[83] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5,2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[84] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[85] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[86] Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data (DataInsider, Sep. 17, 2020), https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data.

[87] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

Health-sector Specific Institutions	Regulation
1. Replicate existing institutions such as the Indian Computer Emergency Response Team (‘CERT’) (National and State level) to operate within the health sector.[88]	1. Develop cyber crisis management plans for all healthcare providers and agencies within the ecosystem.[89] 2. Standardise practices (in a graded manner; where obligations for primary healthcare centres are different from large private hospitals).[90] 3. Develop graded health data sets.

iii. Bridging the Knowledge Gap

It is important to educate stakeholders on how they can operationalise privacy and security standards. Increased awareness through collaboration will allow actors to understand the threat landscape and develop innovative ways of improving privacy and security frameworks. The United States, for example, provides a three tier-model for security and training under HIPAA (physical, technical, administrative).[91] Various organisations train technology security officers using seminars and workshops. Perpetual awareness and education are necessary because of the fluidity of the cybersecurity environment and the inevitable nature of vulnerability. Security professionals continuously monitor the security landscape to learn from breaches in other facilities and prevent and patch similar vulnerabilities in their own facilities.[92]

Reporting mechanisms	Increased awareness
1. Invest in capacity building to highlight and respond to zero-day vulnerability attacks. 2. Collate data on cyberattacks in order to identify vulnerabilities within the system.	1. Conduct an annual ABDM Conference with workshops on data protection, international best practices, data sharing, etc. 2. Share verified and accurate information as soon as possible to counter disinformation.[95]

[88] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[89] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[90] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co-Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

[91] Office of the National Coordinator for Health Information Technology, Guide to Privacy and Security of Health Information,https://www.healthit.gov/sites/default/files/pdf/privacy/onc_privacy_and_security_chapter4_v1_022112.pdf.

[92] Brenna Smith et.al., *Security Techniques for the Electronic Health Records*, 41 J. Med. Syst, 127 (2017).

[95] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

Reporting mechanisms	Increased awareness
3. Develop and enforce uniform reporting standards. 4. Use data acquired through audit trails to identify areas of concern and strengthen the same.[93] 5. Provide victims of identity theft with application and business transaction records about fraudulent transactions made in their names.[94]	3. Take initiative to improve awareness of available assistance initiatives (victim- support, training, and certificate courses that healthcare providers can undertake etc.)[96] 4. Invest in cyber hygiene training and certificate courses to educate healthcare staff.[97] 5. Train cybersecurity professionals to deal with the unique challenges/risks associated with healthcare, including increased familiarity with medical technology.[98]

iv. Graded Health Datasets

Patient health data is usually a broad gradient ranging from highly sensitive data to highly shareable data. Diagnosis of diseases with social stigma is one end while rare disease diagnosis may be the other end, requiring a flexible regulatory regime for maximising benefit to patients and doctors. Segregating data based on risks and the context in which it is collected and used will form the foundation for principles-based regulation based on tiered obligations and access controls for each type of data.

Classification of Health Datasets and Risk Assessments

1. Classify data based on its nature and the risk associated with it. For example: anonymised, non-person or personal data or operational information distinct from personal health records.
2. Conduct risk assessments to identify sensitive categories and define acceptable data practices for each classification.
3. On the basis of such classification, set bright lines for use, storage and sharing of data.
4. Show citizens the classifications of their health data, the associated levels of security, and who has access to their data.

[93] Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data (DataInsider, Sep. 17, 2020), https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data.

[94] Section 609(e), Fair Credit Reporting Act (15 USC 1681), https://www.ftc.gov/system/files/documents/statutes/faircredit-reporting-act/545a_fair-credit-reporting-act-0918.pdf. Federal Trade Commission, 2020 Privacy and Data Security Update, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-securityupdate/20210524_privacy_and_data_security_annual_update.pdf.

[96] The CyberPeace Institute, Playing with Lives: Cyberattacks on Healthcare are Attacks on People (2021), https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf.

[97] Nate Lord, Healthcare Cybersecurity: Tips for Securing Private Health Data (DataInsider, Sep. 17, 2020), https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data.

[98] Nikhil Pahwa, What India Should Do To Improve Cybersecurity In Healthcare — Ambassador Latha Reddy, Co- Chair Of The Global Commission On The Stability Of Cyberspace – #NAMA, Medianama (Aug. 5, 2021), https://www.medianama.com/2021/08/223-improve-cyber-security-healthcare-latha-reddy/.

II. WHERE WE ARE TODAY?

This assessment framework is an attempt to capture the flux of law and policy in digital healthcare. Our aim is to begin with a comprehensive safeguards framework incorporating existing legislations[99], case-laws[100], regulatory norm and results of public and closed-door consultations. We are cognisant of the need to add nuance to the conversations around digital health, temper expectations and focus on the essential prerequisites for successful interventions under the ABDM.

We assess policy requirements at the level of legislation, policy, and the implementation of operational best practices. We suggest a model list of questions that may be used to assess a government digital healthcare system, a policy framework, or a digital healthcare provider.

The framework we designed have the following indicators:

Level	Description
🔴	No framework exists on this topic.
🟡	A draft or pilot framework or legislation exists, with some signs of government activity to address the policy area concerned.
🟢	A definite framework, addressing the policy area concerned, is in place and officially adopted.

[99] Information Technology Act, 2000. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[100] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (hereinafter Puttaswamy I). Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (hereinafter Puttaswamy II).

GOVERNANCE

Does the system have a ‘legitimate’ aim and a targeted social outcome?	According to the 9-Judge Bench in Puttaswamy (2017), a legitimate State aim is the second test for a State intrusion into individual privacy.[101] If the State anonymises individual profiles, it may legitimately assert a valid state interest in “the preservation of public health to design appropriate policy interventions on the basis of the data available to it”.[102]	🟢
Are there adequate checks and balances to government actions?	While the ABDM policy document discusses the need for oversight mechanisms, these have not yet been notified. The NHA is tasked with developing compliance standards and could also develop functional mechanisms or structures that provide checks and balances to government action.	🟡
Have the actors (and their roles) in the digital \ecosystem been clearly delineated?	The ABDM’s Health Data Management Policy clearly identifies different actors, their rights, and their responsibilities. It differentiates between private actors, data fiduciaries, and health service providers.[103] However, since it is not backed by legislation, the government has said in a statement that: “[t]his policy is not to be interpreted or construed as giving any entity or individual rights which are greater than those that such entity or individual would be entitled to under applicable laws”.[104]	🟡
Have the ecosystem’s usecases been clearly delineated?	The NDHB and the ABDM Strategy Overview clearly identify various use cases for digital healthcare and clearly identify the ABDM’s role within thatuse case.[105] A non-exhaustive list of the first set of use cases of the system include queue management, interoperable medical records, possibility of easier second opinion by allowing for swift data transfer. In the future, however, there are bound to be more applications that various stakeholders might use the health infrastructure for. There is immense scope for guidance on how the ecosystem will accommodate expansion in the future.	🟡
Are there adequate efforts to standardise processes, such as reporting requirements, within cybersecurity and otherwise?	At present, there is no standardised format to report cyberattacks. In general, the absence of regulation has led to different institutions following varied sets of standards. Some, for example, follow SNOMED CT for inputs into EHR, some ICD-10 based classification, while some still do not follow any standards at all.[106]	🟡

[101] Puttaswamy I (Plurality, para 182).

[102] Puttaswamy I (Plurality, para 180). The majority in Puttaswamy II notes about the Privacy bench that Chelameswar and Sapre, JJ. have adopted the ‘compelling state interest’ test; Kaul, J., has asked whether the intrusion satisfies the “public interest,” and Justice Nariman adopts the standards in the RTI Act, which provide for the “larger public interest” being satisfied. However, the majority in Puttaswamy II decides to adopt the plurality’s position here, because of the general variance of opinion, the plurality governs and “legitimate state interest” is the governing standard. See Puttaswamy I (Sikri, writing for the majority, para 124).

[103] Gazette Notification, Registered No. DL –(N) 04/0007/2003-18.

[104] Neetu Chandra Sharma, Centre approves health data management policy of ABDM (mint, Dec. 14, 2020), https://www.livemint.com/news/india/centre-approves-health-data-management-policy-of-ndhm- 11607962291863.html.

[105] *See* NDHB, p. 18 (on the anonymizer). *See generally* National Health Authority, ABDM Strategy Overview (2020).

[106] Nikhil Pahwa, What India Should Do To Improve Cyebrsecurity in Healthcare--Ambassador, Latha Reddy, Co-Chair of The Global Commission On The Stability of Cyberspace--#NAMA, Medianama (Aug 5,2021), https://www.medianama.com/2021/08/223-improve-cybersecurity-healthcare-latha-reddy/.

CYBERSECURITY

Is there a mitigation strategy in place in case of failure or coordinated attack on the data systems?	The Health Data Management Policy states that ‘[t]he NDHM shall issue appropriate technological and operational guidelines providing for the establishment and maintenance of the federated architecture, for ensuring the security and privacy of the personal data of data principals, and for maintenance of electronic medical records and electronic health records’.[107] These technological and operational guidelines have not been issued.	🟡
In the effort to improve cyber hygiene, have any investments been made in information sharing mechanisms?	The Indian Computer Emergency Response Team (‘CERT’) have issued ‘security tips for common users’ that can be accessed on their website.[108] However, most people are not adequately informed of the dangers of cyberattacks or the importance of their right to privacy. Targeted efforts to combat disinformation will also play a significant role in educating citizens on any malware attacks.	🟡

DATA PROTECTION

Is there a national data protection law in place?	At the moment, there is no legislation for data protection. However, the Personal Data Protection Bill, 2019 was referred to the Joint Committee of Parliament (‘JPC’) in 2019.[109] Following its fifth extension, the JPC tabled its report on the Bill in the Parliament’s Winter Session of 2021.[110] Protection of personal data and sensitive data is currently covered under the IT Act and the SPDI rules. There remains significant scope to increase data protection at scale.	🔴
Does the law clearly define the kinds of data that will be collected?	The ABDM’s Health Data Management Policy distinguishes between EHRs, EMRs, personal data, and sensitive personal data.[111] The policy framework, could be buttressed with more information about the metadata that will be collected and about the use of such data in policymaking or governance.	🟡
Are there privacy by design systems that minimise the harms from a data breach?	While the Health Data Management Policy (“HDMP”) published by ABDM lays down privacy by design as a guiding principle in building the system, there are lingering concerns of effectiveness of the protections in the absence of relevant legislation. The policy could have	🟡

[107] NDHM Health Data Management Policy, para 26.3.

[108] Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team, https://certin.org.in/.

[109] Ministry of Parliamentary Affairs, Joint Committee on the Personal Data Protection Bill, 2019 seeks views and suggestions (Feb. 3, 2020), https://pib.gov.in/PressReleasePage.aspx?PRID=1601695.

[110] Joint Committee on the Personal Data Protection Bill, 2019 (2021) http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

[111] NDHM Health Data Management Policy, para 26.3.

	improved its engagement with the large-scale processing of data that could happenin the absence of a data protection law. Moreover, in case of a breach, the provisions of the HDMP in addition to mandating disclosure of breaches to the NHA, could also mandate discloser to the user.	
Are policies regarding best practices in the collection, use, and retention of sensitive data laid down?	As it stands right now, these practices are not defined, and standards are yet to be prescribed. While implementing ABDM through the various states, these aspects must be laid down, policies must be standardised and redlines must be clearly demarcated. For example, secondary use of data must happen within a defined framework that respects rights and user agency. Some activities that are prohibited must be defined. For example, sharing of data for advertising, marketing, insurance, etc.	🟡

COMMUNITY

Is there a time-bound system to offer compensation as well as remedies for victims who have suffered significant harm?	The onus of developing a system with such safeguards seems to rest on private providers. According to the ABDM Sandbox Guidelines, applicants are required to present plans which adequately protect consumers, including disclosures, risk management, incident reporting, redress, insurance (victim compensation funds), etc.[112] Further guidance is necessary in order to ensure that citizen interests are protected, especially given the ambiguity of the status of healthcare in the Consumer Protection Act, 2019.	🔴
Has community participation been institutionalised under the relevant Ministry?	No, community mobilisation has not been institutionalised at the Central or State level.	🟡

[112] ABDM Sandbox Guidelines, para 6.7 (available at https://abdm.gov.in/publications/sandbox_guidelines). 113 This decision dates back to the National Health Policy, 2017

MISCELLANEOUS

Is the use of the data ecosystem by private actors effectively regulated?	Yes, authentication takes place through Aadhaar under the framework contemplated by the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020,[113] and all data storage andsharing takes place through the ABDM backend and the Unified Health Interface.	🟢
Is there a common standard for graded datasets, based on a risk assessment, laid down in the policy framework?	The ABDM Strategy Overview provides for classification of data as personal and non-personal, [114] while the UHI consultation paper also provides for aggregated and anonymised data.[115] However, the risk assessment conducted is limited to data sharing practices and does not extend to cybersecurity frameworks.[116]	🟡
Is there a detailed manual for stakeholders to sensitise to best practices in data, such as how to grade data at source?	While there a detailed manual for healthcare professionals has not been issued at present, the HDM Policy requires all data fiduciaries to ensure that ‘training and awareness materials around data protection and privacy are developed for its employees and data processors’.[117] The HDM Policy also requires role-based training as well as periodic training and awareness programs at which attendance is recorded for auditing and documentation.	🟡
Are the building blocks within the ecosystem, including identification, codified in a valid law?	There is no legislation that governs health-care related identification. However, there is some policy guidance. For example, The National Resource Centre for EHR standards provides for patient identifiers.[118] Additionally, there are certain special circumstances under which merely identifying that a particular individual is a patient can be a violation of the Code of Medical Ethics Regulations, 2002.[119]	🔴
Are there effective alternatives to using foundational IDs like Aadhaar for access to welfare service delivery?	The ABDM currently supports registration for a Health ID with either Aadhaar or a phone number.[120] However, there are instances where exclusion can be amplified when alternates to digital mode of authentication are not expressly laid down.	🟡
Are there effective civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use of data?	Yes, the ABDM has a web-enabled system that is designed to resolve issues arising out of the building blocks of the ABDM.[121] It allows users to file grievances, communicate with the Grievance Redressal Officer directly, provides for an application number and status tracker. However, it is not accessible in local language and does not have screen reader capabilities. Access details to the call centre/postal address is also only provided on the website. Therefore, it remains inaccessible to several groups.	🟡

[113] This decision dates back to the National Health Policy, 2017.

[114] ABDM Strategy Overview, p. 9.

[115] UHI Consultation Paper, p. 22.

[116] Health Data Management Policy, Clause 27.

[117] Health Data Management Policy, para 27.2(h).

[118] National Research Center for EHR Standards, Patient Identifiers (last available on Sep. 3, 2021), https://www.nrces.in/standards/government-of-india-standards/patient-identifiers.

[119] Indian Medical Council (Professional conduct, Etiquette and Ethics) Regulations, 2002. See also N.N. Mishra et al., *Privacy and the Right to Information Act*, 2005, 5 Indian Journal of Medical Ethics 158 (2008).

[120] ABDM FAQ, https://abdm.gov.in/home/faq.

[121] Ayushman Bharat Digital Mission Grievance Portal, https://grievance.abdm.gov.in

The Dialogue™

INFORM ENGAGE IDEATE

Recommended Citation : S. Chatterjee, K. Venkatesh, E. Vaidya (2022) ***India's Digital Health Dreams: Getting it Right*****, The Dialogue™**

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

https://thedialogue.co