Ethics in Digital Public Infrastructure: A case study of India's health DPI approach

Anita Gurumurthy | IT for Change

Session on Human Rights Protocol Considerations, IETF

21 March 2025

Table of Contents

What is Digital Public Infrastructure?

DPI is an umbrella term used to describe a range of technological systems (digital identity, data sharing systems, digital payments, etc.) seen as “essential capabilities for participation in society and markets as a citizen, entrepreneur, and consumer in the digital era.” (Co-Develop 2025)

The term has been used to refer to a variety of initiatives from grassroots social media platforms to state-promoted interfaces for delivering welfare payments.

The UNDP notes that DPI involves some combination of

(i) networked open technology standards built for public interest,

(ii) enabling governance, and

(iii) a community of innovative and competitive market players working to drive innovation, especially across public programs

India's approach to DPI

The India DPI approach has garnered international attention for innovations in the delivery of social welfare as well as the economy.

In the last few years, India has rolled out:

- Aadhaar (the digital identity system);
- the Unified Payments Interface (UPI - an instant, interoperable, payment system);
- Open Network for Digital Commerce (ONDC - a discovery and fulfillment network for e-commerce);
- the API Setu initiative (which provides open Application Programming Interfaces for public service delivery) and
- sector-specific data exchanges for third party data sharing in key development domains such as health, agriculture, and urban development.

Ayushman Bharat Digital Mission (ABDM)

The Healthcare DPI in India

Ayushman Bharat Digital Mission (ABDM): The Healthcare DPI

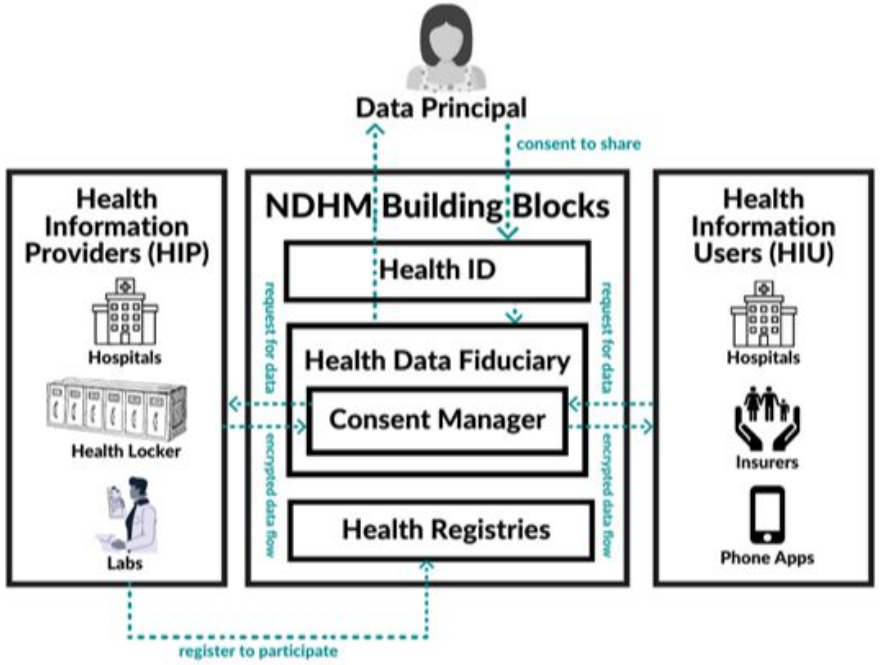
- Launched in September, 2021 with the objective of "**developing the backbone necessary to support the integrated digital health infrastructure of the country [...] to bridge the existing gap amongst different stakeholders of the healthcare ecosystem through digital highways".**
- The vision is to enable the "frictionless" exchange of health data in order to incentivize private sector health innovation to address the country's public health challenges.

Ayushman Bharat Digital Mission (ABDM): Building Blocks

Core building blocks of ABDM include:

1. **Digital Health ID** to access and share personal digital health records.
2. **Health Facility Registry** to access a comprehensive repository of health facilities across the country, including pharmacies, imaging centres etc.
3. **Health Professionals Registry** to access a comprehensive repository of all health professionals across modern and traditional systems of medicine.
4. **Unified Health Interface,** a framework of open protocols that enables an interoperable network of health services applications to function with seamless data exchange between various health service providers (hospitals, clinics, labs, pharmacies, insurers, wellness centers, health tech companies, third-party administrators for health insurance, and so on).
5. **Digital Health Application** to enable the management and maintenance of health information via smartphones.

Ayushman Bharat Digital Mission (ABDM): Data Flows



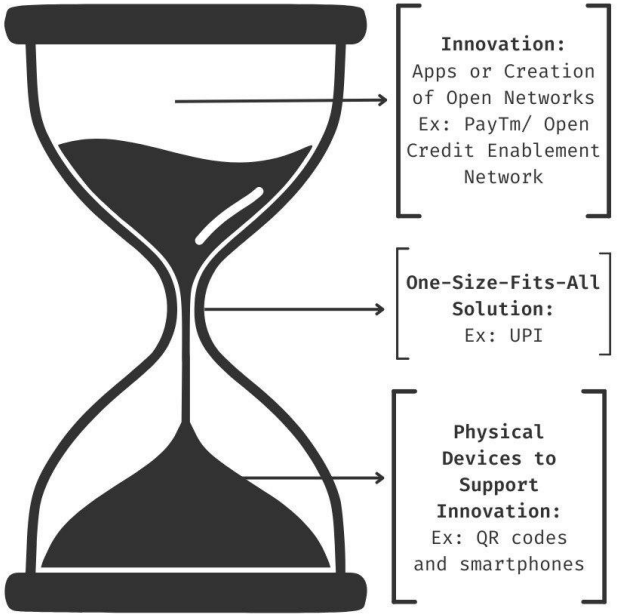
- The data principal holds a unique health ID which grants them access to the repository of their health data.
- Via a consent manager, the patient can consent to the sharing of their health data with Health Information Providers (doctors, hospitals etc.) and Health Information Users (insurance providers, phone apps etc.)
- Health registries (facilities, professionals) effectively carve out *who* the actors are within this digital health ecosystem.

Source: R. Radhakrishnan, Health Data as Wealth: Understanding Patient Rights in India within a Digital Ecosystem through a Feminist Approach

Ayushman Bharat Digital Mission (ABDM): System Architecture

System architecture mimics an 'hourglass' (see image).

The state provides the "essentials" through the development of standards and protocols for platforms, such as the Unified Health Interface. Private entities may build targeted services on top of this.

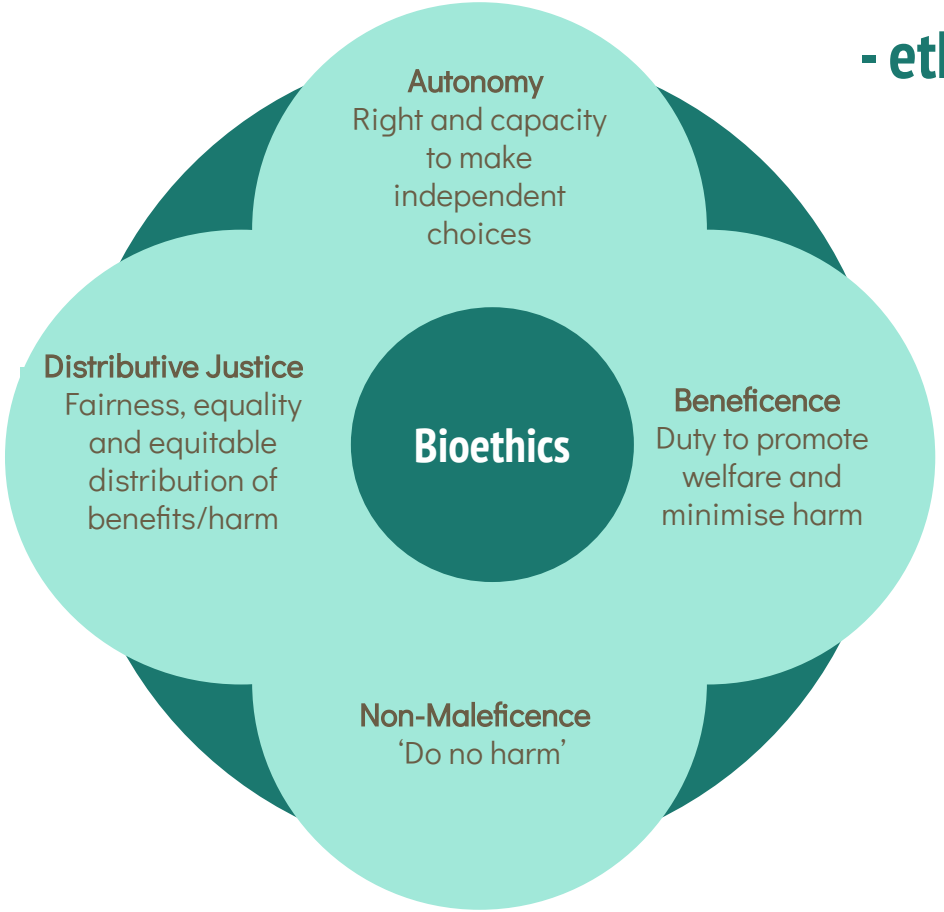


Source: Nandan Nilekani & Viral Shah, Rebooting India

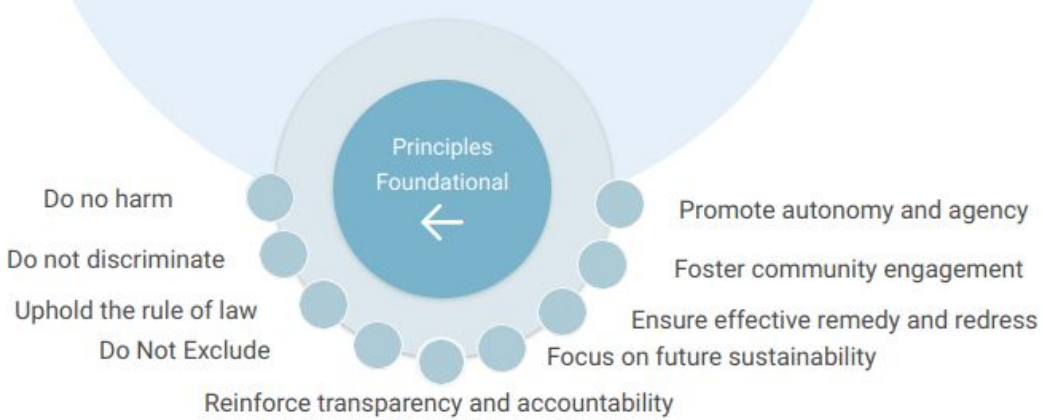
Taking stock of ABDM's ethics baseline and its operationalisation

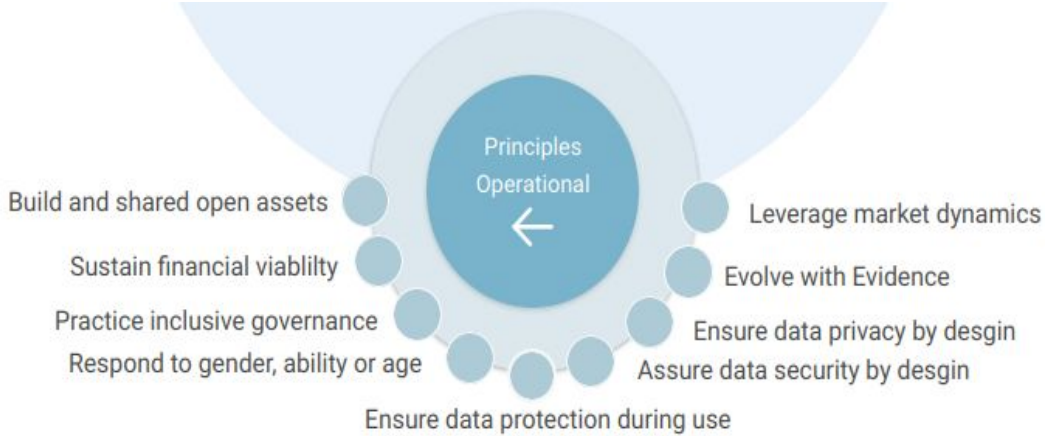
Through the bioethics lens and UNDP's DPI safeguards framework

Bioethics Framework - ethical baseline



Actionising the ethical baseline: Design principles - UNDP





Bioethics Principle 1. Non-maleficence - Do no harm

The data ecosystem of the ABDM lacks an effective data governance framework. Neither the Digital Personal Data Protection Act nor the Health Data Management Policy have instituted any safeguards for the use and re-use of anonymized data.

Operationalising Non-Maleficence

How foundational principles fare

No rule of law framework to ensure:

- Do no harm
- Do not discriminate
- Do not exclude

How operational principles fare

'Privacy by design' principle translates into 'data blind consent managers' in data exchange

Data security translates into encryption in data exchange.

What about the risks of predatory downstream data practices that lead to de-anyonymisation or group profiling?

Who is responsible for a data breach?

Bioethics Principle 2. Beneficence - Promote wellbeing

ABDM expands health data collection and processing to include medical data generated in clinical settings and non-medical data (through Aadhaar-linkage) by private service providers and furthers the commoditisation of health care.

The insurance-led model already has made treatment, particularly in secondary and tertiary care, diagnostic-heavy to justify course of treatment, in some cases solely for the benefit of insurance providers...[thus] increasing cost of care.

“Health datafication will only lead to more of it, where more and more parts of care will be preconditioned... on the data itself, and access, affordability of care will be affected. Denying or delaying treatment preconditioning on access to data... could lead to suboptimal outcomes”

- Public interest technologist, cited in Radhakrishnan, R. Health Data as Wealth: Understanding Patient Rights in India within a Digital Ecosystem through a Feminist Approach

Operationalising Beneficence

How foundational principles fare

- Effective remedy and redress may be compromised in commoditisation
- Compass shifts from centering health as a public good to promoting data markets

How operational principles fare

Openness and interoperability of data seen to be inherently beneficial. Combining clinical and non-clinical data may compromise beneficence by opening up market interests in public services.

Also, brings questions to the fore of how data protection frameworks need to move beyond categories of sensitive personal data. Any data could become sensitive potentially in interlinking. Data is what data does.

The *Indian* hospital industry accounts for 80% *of* the total *healthcare system in India and* was valued at US$ 132 billion in 2023.
Public health care budget is 2% of the GDP

Bioethics Principle 3. Autonomy - ability to make choices

Patients must register with the ABDM data architecture in order to avail of healthcare services. Service provision is based on coercive data collection.

For instance, India's flagship health insurance scheme, the PM-JAY, requires registration with India's foundational ID, Aadhaar. The PM-JAY website does not permit registration using any other government ID (more on PM-JAY in the subsequent slides)

This reflects a clear State push towards establishing Aadhaar as the foundational identity layer—a vision central to several DPI initiatives.

However, access based on '*no data fee, no service*' severely undermines individual and collective autonomy.

Several do not have access to Aadhaar cards, for instance people with chronic diseases, like leprosy or people with disabilities struggle with Aadhaar enrollment and authentication, leading to exclusion of those in need of healthcare services, diluting their right to equitable access to healthcare.

The prospect of sharing health data in this manner also deters some from accessing digital healthcare at all. For instance, patients of diseases with social stigma, such as HIV-AIDS would be excluded from this digital ecosystem, severely diluting their individual and collective patient autonomy.

Bioethics Principle 3. Autonomy - ability to make choices

- Doctors play a critical role in building individuals' electronic health records. They must record the patient's symptoms, diagnoses and prescribed treatment. Several Electronic Medical Records, however, require data collection through a drop-down menu option. For instance, the next set of options will depend on whether the doctor has chosen "headache" or "leg pain" as the primary symptom. Boxes permitting text entries are often missing in such techno-designs.
- There is a concerted effort towards building interoperable datasets, all of which require data to be entered in a standardised manner. The subsequent linkages across datasets are critical towards building a rich health data market.
- **The power of decision-making is entirely taken away from doctors** , also leading to a **reduction in quality care for patients (implicating beneficence)**

Operationalising Autonomy

How foundational principles fare

- Mandatory linking of Aadhaar (data fee for health service) undercuts autonomy and agency - both individual and collective

How operational principles fare

- Violates the ‘privacy by design’ principle
- In-built choices in diagnosis prevent patient-centricity, privileging standardised data sets

Bioethics Principle 4. Distributive justice - fairness, equity

The Govt of India's health insurance scheme aims to ensure financial protection for accessing secondary and tertiary care from public and private providers – covering 40% of the poor and vulnerable population of the country.

Given the poor state of health care infrastructure, health insurance becomes a modality to direct private investment towards geographies where there are very few providers.

But the real beneficiaries are not those in need.

Insurance companies use the Aadhaar-seeded beneficiary database of the ABDM – which is a goldmine, considering it allows access to different data sets through the UHI, and also receive a huge subsidy from the state in the name of health services.

Operationalising distributive justice

How foundational principles fare

Rule of Law to recognize health data as a public good is absent

Failure to manage market dynamics in a manner that generates public value from health data

How operational principles fare

Interoperability and openness misused for predatory markets

Concluding thoughts

“Architecture is policy” - suggests that architectural design and planning reflect and shape societal values, goals, and outcomes impacting the built environment and influencing public life.

DPI techno-design choices can either uphold/vitiate rights-based ethics. It can create a society that can make public services access a universal right or it can contractualise and privatise access.

Assumptions about tech and innovation are at the heart of social adoption of tech. (In the case study we discussed how public health values, goals and outcomes are being reshaped.)

Technological principles cannot be valorised in and of themselves (**eg. openness, interoperability and scalability**) - whether they further ethics depends on contextual application.

Rule of law cannot be substituted by tech protocolisation. Institutional safeguards are as important as design safeguards.

Thank you!

Other insights?

Questions?