Building Digital Ecosystems for India
From Principles to Practice

An Implementation Blue Book

March 2022

AUTHORS

Aishwarya Viswanathan, Deepro Guha and Bhavani Pasumarthi

RESEARCH LEAD

Rohit Kumar

Contents

Preface

Over the last decade, India has pioneered a new approach to building GovTech - one which prioritises the creation of technology 'building blocks' that multiple innovators can leverage to build citizen-centric solutions: in other words, an approach that focuses on creating open ecosystems instead of closed systems. This approach recommends the use of Free and Open Source Software (FOSS), open standards, and open APIs and encourages interoperability. By doing so, it allows different systems to talk to each other seamlessly, empowers stakeholders, distributes the ability to solve complex societal problems and unleashes innovation to enhance service delivery. Starting with Aadhaar, India has built a menu of such digital solutions that today includes eKYC, DigiLocker, a Unified Payments Interface (UPI) and many other sector-specific solutions.

Three interrelated concepts: NODEs, Public Digital Platforms and IndEA

The Ministry of Electronics and Information Technology (MeitY), on behalf of the Government of India (GoI), has been a key advocate and custodian of this approach, putting forth three interrelated concepts – India Digital Ecosystem Architecture (IndEA) Framework, Public Digital Platforms and National Open Digital Ecosystems (NODEs).

The India Digital Ecosystem Architecture (IndEA) Framework provides a set of architectural principles, reference models and standards to support the seamless flow of data across government departments. Leveraging these principles, India has made tremendous strides in building critical Public Digital Platforms such as Aadhaar and UPI which have also facilitated the creation of National Open Digital Ecosystems (NODEs).

All three concepts adopt architecture thinking and interoperability – The IndEA Framework at a 'whole of government' level, and Public Digital Platforms & National Open Digital Ecosystems at the sectoral or segment-specific level. They build on common tech elements and strive for one common outcome – namely adopting a de-siloed approach to GovTech, to unlock greater economic and societal value for the citizen.

The strategy for NODEs consultation white paper, released in early 2020, and the latest IndEA 2.0 draft framework have both generated wide public interest and engagement. It is now timely to take this approach forward by codifying the details into an implementation blue book so that the adoption of the IndEA & NODE approaches can be mainstreamed across various sectors and simplified for all government departments. This is what this document aims to do.

Acknowledgements

This study has been authored by Aishwarya Viswanathan, Deepro Guha and Bhavani Pasumarthi along with Rohit Kumar. The authors are a team of researchers from The Quantum Hub (TQH), a public policy research and communications firm based in New Delhi.

The study would not have been possible without the inputs and generosity of stakeholders within the government and civil society who shared their time and experience with the research team. In particular, we would like to thank Varad Pande, Kriti Mittal and Twinkle Malhan of Omidyar Network India for sharing insights based on their previous work on Open Digital Ecosystems, and to Tushar Goel, Kushal Wadhawan and Deepika Raman of the International Innovation Corps (IIC) for their inputs and feedback on the early drafts of the study.

Acronyms

- GoI – Government of India
- FOSS – Free and Open Source Software
- MeitY – Ministry of Electronics and Information Technology
- NODE – National Open Digital Ecosystem
- UPI – Unified Payments Interface
- IndEA – India Digital Ecosystem Architecture
- ABDM – Ayushman Bharat Digital Mission
- NUIS – National Urban Innovation Stack
- NDEAR – National Digital Education Architecture
- PDPB – Personal Data Protection Bill
- GDP – Gross Domestic Product
- ICT – Information and Communication Technology
- NeGP – National e-Governance Plan
- SSO – Single Sign-On
- GSTN – Goods and Services Tax Network
- MoHUA – Ministry of Housing and Urban Affairs
- API – Application Programming Interface
- PSP – Payment Service Providers
- MSME – Ministry of Micro, Small and Medium Enterprises
- IUDX – India Urban Data Exchange
- MVP – Minimum Viable Product
- SPV – Special Purpose Vehicle
- GeM – Government e-Market Place
- NPCI – National Payment Corporation of India
- OGD – Open Government Data
- PGR – Public Grievances and Redressal

Digital Ecosystems: New Paradigm of 'GovTech'

The world is at the cusp of a paradigm shift in the way digital solutions are being deployed for large-scale societal impact. Technology interventions such as interoperable digital platforms, open standards and protocols, and open APIs, can now enable service delivery at population scale, while opening up new opportunities for entrepreneurs and innovators. India is today at the forefront of this movement. As a country, we are building critical national level tech infrastructure in sectors such as health (Ayushman Bharat Digital Mission), agriculture (India Digital Ecosystem of Agriculture), urban affairs (National Urban Digital Mission), education (National Digital Education Architecture) as well as in areas such as justice. Many state governments are also adopting a platform-based approach to enable seamless delivery of welfare benefits and public services to citizens. With projects like the *Modular Open Source Identity Platform* (MOSIP) and Digital Infrastructure for Vaccination Open Credentialing (DIVOC), we are today also building 'made in India' population scale tech solutions for the rest of world.

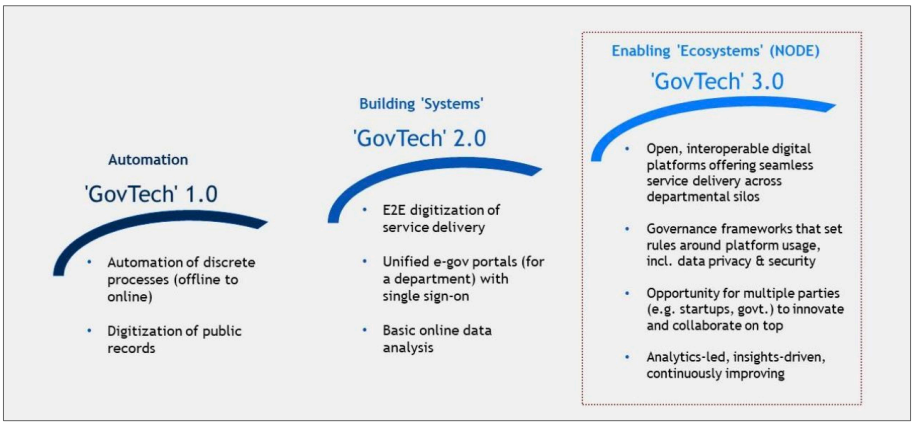
India's GovTech approach, i.e., its use of technologies to create efficient and transparent systems in public service delivery has evolved over the past few decades. We started with 'GovTech 1.0' which called for the 'automation' of processes, such as raising service requests or viewing the status of applications online. From here we moved to 'GovTech 2.0' which represented 'building systems' i.e., end to end digitization of service delivery. Examples of such interventions included the Government e-Marketplace (GeM) to provide digitized and streamlined end to end services for public procurement – where buyers and sellers can transact with each other through a single-window, instead of going through multiple portals.

Today we are embracing 'GovTech 3.0' which leverages the increased digitization of service delivery, and focusses on breaking silos to create 'enabling ecosystems'. The Ayushman Bharat Digital Mission (ABDM) is an example of such an ecosystem that aims to create the digital infrastructure necessary to connect all stakeholders in healthcare. This approach to public service delivery takes a holistic view of the many elements (like IDs, core registries, data exchanges etc.) in the digital ecosystem including their interlinkages, rather than following the traditional 'monolithic tech systems' approach.

The 'enabling ecosystems' approach is a key element of both the India Digital Ecosystem Architecture (IndEA) Framework and the strategy for the NODE consultation white paper. Other unifying and defining characteristics of the IndEA and NODE frameworks include envisioning:

- The government as an enabler, rather than an end-to-end service provider, with a focus on creating the base digital infrastructure that can enable innovators to build solutions on top.
- The government as a regulator for ensuring accountability and protecting the rights of the individuals.
- Collaboration between the public and the private sector for designing *demand driven* user-centric solutions rather than *provider driven* solutions.

- An empowered community of users and innovators with tools to participate in the new digital ecosystems, while being able to demand accountability.



Evolution of GovTech[1]

Understanding Digital Ecosystems:

The ecosystem approach to developing digital infrastructure requires that we go beyond the tech itself, to look at how it interacts with its users. In particular, it draws attention to three critical components to ensure that *user-centricity* and *responsibility* remain key hallmarks to the adoption of digital solutions:

- The technology (or the digital platform) at the core, anchored by
- A robust governance framework, and
- A vibrant community of actors engaging with the platform and working together to building solutions to deliver shared value.

The technology or the digital platform is the 'tech' layer, while the governance frameworks and the community are the 'non-tech' layers. Together, they can help create a robust digital ecosystem.

Technology layer

This layer comprises the core technology infrastructure that includes components such as data registries, data exchanges, open APIs, open standards and protocols etc. By allowing for openness in the design, the tech allows for innovators to build innovative solutions and facilitate the delivery of services to the intended user base.

Community layer

A vibrant community of partners is the driving force of any digital ecosystem. This includes builders (public and private institutions, start-ups, developers), end-users (consumers of the digital services) and facilitators (private and public entities that finance development, drive adoption, ensure last-mile access and maintain oversight).

[1] Image source: NODE consultation white paper, 2020

Governance layer

A digital ecosystem typically comprises multiple stakeholders - institutions that own the digital platform, co-creators who develop solutions on it, and individuals who consume services and/ or participate in designing solutions. The governance layer therefore refers to the framework which establishes the rules of engagement between all the stakeholders in the ecosystem, and ensures institutional accountability, transparency, and enables fair and equitable outcomes for all.

Leveraging the ecosystem approach: Unleashing the potential of digital ecosystems while mitigating risks

GovTech 3.0's digital ecosystem approach has the potential to unleash economic and societal value in distinct contexts. By breaking down data silos and creating shared digital infrastructure, service delivery models can be reinvented to create greater access for underserved populations, while reducing transaction costs and inefficiencies.

It is estimated that by 2030, 10 high potential digital ecosystems in sectors like health, education, agriculture, skilling, logistics, MSME etc., can unlock economic opportunities equivalent to USD 500+ billion (INR 35+ lakh crore) - roughly 5.5% of India's Gross Domestic Product (GDP), while generating an additional USD 200+ billion (INR 15+ lakh crore) in savings for the country.[2]

Moreover, sector-specific digital ecosystems, such as the one for MSMEs, can secure societal benefits in the form of improved access to institutional credit for small businesses, which can, in turn, result in the inclusion of 10 to 20 million MSMEs in the formal financial system (approximately 40-50% of MSMEs with unmet credit needs). Similarly, in the Talent sector, an interoperable platform that brings together information about employment opportunities, job-seekers, and skills can potentially match 50 to 80 million people with better-fit jobs (approximately 10-20% of the non-casual labour force).[2]

The potential is undoubtedly immense. However, there are also challenges that accompany the development of digital ecosystems, and that developers and policymakers must systematically guard against.

Identifying and mitigating risks

Digital ecosystems represent a paradigm shift from the older, ICT-based public service delivery models, but the scale of operation also heightens the need for greater safeguards. In particular, there is a need to guard against the following risks:

a. **Data centralisation risk:** Digital ecosystems break down data silos, creating a 'single source-of-truth' for all relevant stakeholders, wherein the same underlying data is shared for service delivery. For example, the IndEA 2.0 draft report highlights the role of federated architecture and emphasises constructs such as Single-Source-of-Truth and System-of-Records. However, the aggregation of data (particularly when it is personal in nature), can create risks that must be handled appropriately. Also, it is important to consider that if the data is incomplete or erroneous, it could lead to faulty decision-making. While this problem would have affected databases in the past as well, these were distributed in nature, thus reducing the risk of consistent exclusion across databases.

[2] ONI-BCG Report on Building India's Digital Highways. https://opendigitalecosystems.net/pdf/ODE-Report.pdf

Given the data centralisation risk, there is a critical need to build mechanisms and processes that allow users to correct, complete, and update misleading, incorrect, and out-of-date personal data to ensure data quality. The CoWIN platform is an example of a system that has now developed an error correction mechanism, allowing users to log-in and rectify any inadvertent errors in their vaccination certificates.

Another related risk is the potential misuse of aggregated data. A single point of failure can emerge in centralized registries, increasing their vulnerability to cyberattacks. Also, without safeguards, interoperability across multiple data registries could put an individual's privacy at risk. Given these issues, privacy-by-design principles and appropriate security measures must be built into the platform design, for example, through E2E data encryption, purpose specification, data minimization, electronic consent and authorization frameworks, etc. Initiatives such as penetration testing or bug bounty programs can help also identify and address security vulnerabilities in platforms, while simultaneously increasing interest in developing digital ecosystem architectures.

In cases of actual data breaches, related safeguards must be put in place through clear grievance redressal mechanisms and accountable institutions.

b. **Exclusion risk:** As highlighted in the IndEA 2.0 draft report, ensuring universal access is a key cornerstone of co-creating an inclusive digital architecture. In order to operationalise this ideal, digital exclusion errors must be addressed. In India, these errors are driven largely by a lack of access to technology infrastructure, as well as limited digital literacy among marginalised groups.

According to NITI Aayog's Sustainable Development Goals (SDGs) India Index 2020-2021 report, out of every 100 people in India, 55 have an internet connection. The latest (2019-21) National Health and Family Survey (NFHS-V) data also shows that access is not uniformly distributed among different groups. In terms of the gender divide, against 57.1% men who have ever used the internet, only 33.3% women have ever accessed it. Similarly, the urban-rural gap is significant, with rural women being the most disadvantaged among the groups, and urban men having the greatest access. Only 24.6% of rural women have ever accessed the internet, against 72.5% of urban men. Such gaps in access can exacerbate inequalities, impacting the efficacy of digital public service delivery.

Closing the digital gap is not an easy task, but certain measures can be taken to bridge it slowly. One such measure is the provision of last-mile access and engagement for rural and marginalised groups, through multi-modal, omni-channel access (mobile, web, etc.) — online and offline — in order to account for different levels of tech know-how. Similarly, user-friendly, vernacular interfaces with disability-friendly options can help widen the net of citizen participation considerably. Developing mass awareness programmes while encouraging intermediation by local community groups can also help encourage greater participation.

c. **Adoption Risk:** The success of a digital platform relies on its adoption by innovators who can take advantage of the infrastructure to build services as well as the use of those services by a wide community of users. Without adequate adoption, the digital platform could quickly lose its utility.

   To ensure adoption, the quality of underlying datasets is the first risk that must be guarded against. Open data platforms sometimes contain compromised datasets or datasets in non-usable formats. This can make it challenging for the developers to leverage these datasets to offer services. Ensuring transparent data governance, that is, clear publication of data sources, ownership, policies/standards for data collection and storage, etc., can help ensure good data quality.

   NITI Aayog's National Data and Analytics Platform (NDAP) is one such initiative that aims to improve access to publicly available government data through an intuitive portal tailored to the needs of a variety of stakeholders. The project's Vision Document mentions not only the setting up of clear Standard Operating Procedures (SOPs) for data updation, but also a compliance tracking exercise for them. It also states that data will be provided in a machine-readable format with customisable analytics, thereby providing a unique value proposition to all innovators.

   To ensure adoption, it is also important to undertake focused initiatives to generate awareness and incentivize usage by both co-creators and users. Unless a critical mass of applications and users is brought together, it is unlikely that the digital platform will gain the momentum that it needs to scale.

d. **Operational Risks:** In the absence of a forward-looking design and operational strategy, systems and platforms run the risk of becoming obsolete rapidly. Particularly from the perspective of longevity, all builds must be flexible enough to address not only immediate but also future needs. Therefore, in order to create a holistic ecosystem, operational challenges such as those related to third party procurement and contracting, on-boarding technology talent and required capabilities, and financing must be addressed upfront by institutions that are developing these ecosystems.

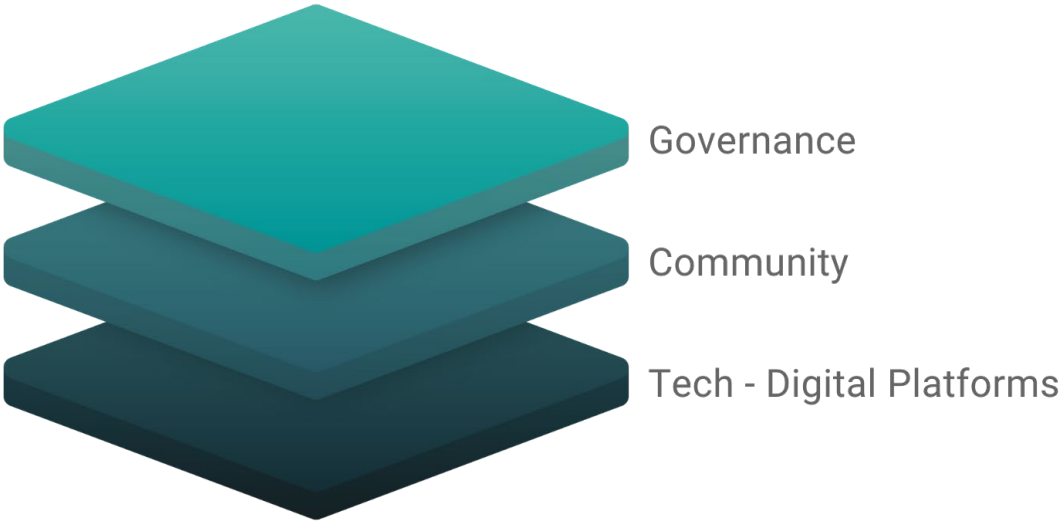
Given the potential that digital ecosystems hold and the challenges that may come with their implementation, it is important that key guiding principles of IndEA and NODE are kept in mind as different ecosystems are operationalised. This will ensure that upcoming digital ecosystems protect the rights of users, create accountability, incentivize innovation and ultimately deliver user-centric services.

The design specifications and policy criteria covered by this implementation blue book attempt to highlight how various stakeholders can adopt these principles in practice to suit their contextual needs. In particular, the blue book can be utilized by a broad range of stakeholders including (1) the institutions that build, deploy, operate, maintain, and scale digital ecosystems; (2) policymakers responsible for setting up governance

frameworks; and (3) civil society actors looking to strengthen delivery of public services through digital platforms.

Operationalizing robust Digital Ecosystems

The Strategy for National Open Digital Ecosystem (NODE) Consultation Whitepaper outlines 15 guiding principles across 3 categories namely, technology (digital platforms), governance and community engagement. The India Digital Ecosystem Architecture (IndEA 2.0) illustrates a set 27 principles across 5 categories, namely ecosystem, architecture, business, technology and governance that actors in the ecosystem can adopt. This implementation blue book, unpacks the 15 principles listed in the NODE Consultation Whitepaper as well as the 27 principles listed in IndEA 2.0 draft into 45+ 'sub principles' to highlight specific design elements and policy choices that can help operationalize a digital ecosystem.



While the NODE and IndEA 2.0 design principles provide high level guidance, the sub-principles presented here are meant as a 'how to' guide to help builders put these principles into practice. The blue book also includes a set of illustrative examples to show how these principles can be brought to life by discussing best practices from within India and abroad.

The hope is that this framework will assist the many actors involved in the development of digital ecosystems to realize the benefits of the IndEA and NODE approach while mitigating potential risks.

Principles for Designing Digital Platforms

Principle 1: Be open and interoperable

Digital ecosystems must seek to build their respective digital platforms *on* open-source and *as* open-source. Use of open technologies, including open source software is crucial for ensuring vendor neutrality, transparency and strategic control of the core digital infrastructure. The flexibility and cost-effectiveness offered by open source allows for creation of customised solutions that are tailored to local contexts, and helps facilitate wider community collaboration that in turn drives innovation. In this regard, upcoming digital ecosystems may adopt and conform to MeitY's Open Source Software Policy to the extent possible.

Additionally, under the proposed federated models that IndEA 2.0 and NODE seek to further, open source technologies must be complemented with the use of open standards, APIs and specifications. This will help unlock 'interoperability' i.e., where data can be exchanged and used across multiple applications and systems (with consent as necessary) - thereby enabling solutions both within and across upcoming digital ecosystems to work in a unified manner.

For this, specifications that digital ecosystems adhere to must align with MeitY's Policy on Open Standards and Policy on Open APIs.

Sub-Principles:

1.a. Free and Open Source Software (FOSS): Use building blocks that are 'free' and 'open source' i.e., software that is freely licensed to use, copy, study, change, improve, and redistribute for building the core/base infrastructure of a NODE.

> **Example 1:** As the CoWiN application, India's central vaccine administration and credentialing system was built using open source DIVOC software, a community of collaborators were able to access the source code and come together to resolve issues that came up in implementation, such as when the application was printing the incorrect age on vaccination certificates.[3]
>
> **Example 2:** DigiLocker, a flagship initiative of the Ministry of Electronics & IT (MeitY) under the Digital India programme, provides a 'digital wallet' and acts as a secure document exchange platform. The DigiLocker has also been built using open source programming languages including PHP and Python and tools like Node.js.

1.b. Source code available in the public domain: Release the source code of the base infrastructure layer[4] (except those that are notified as sensitive), for anyone to inspect. Source

[3] https://www.livemint.com/news/india/error-in-your-vaccination-certificate-you-can-now-rectify-it-on-cowin-here-s-how-11623212076161.html

[4] Note: We distinguish between the base digital infrastructure layer and applications built on top of it. Applications may be built by innovators using open APIs and they may or may not release source codes in the public domain, especially when these applications are built outside the Government

code, that is stored in a public repository and shared publicly will allow visibility into the functioning of the code and facilitate auditability.

> **Example:** Estonia's Public Codes Registry allows anybody to access and use the open source code unless required otherwise for security reasons.

1.c. Open licenses: Grant permissions for anyone to use and/or share the code of the base digital infrastructure layer freely under either of the two types of licenses:

- *Copyleft license* that grants use rights but forbids proprietization and requires all derivative works to be subject to the original license.
- *Permissive license* that grants use rights, including right to re-license. Allows proprietization and mixing/ combining of software components with different licenses.

Adopting open licenses can help amplify impact by creating public goods, by allowing for the use of the developed code in other contexts and/or facilitating improvements. To ensure the selection of right licenses, it is integral that the interests of all stakeholders - communities, businesses, academia and governments - are taken into account to enable significant contributions from all spaces to co-create a thriving open ecosystem.

In this regard, refer to DPGA's take on approved licenses for Digital Public Goods and additional resources on Open Source Licenses.

1.d. Open standards: Ensure application-design is technology independent and follows standards (technical criteria, methods, processes, practices etc.) that are made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. This will ensure that the standards maintain interoperability and quality.

While designing standards, consider MeitY's policy on open standards for e-governance, the manual on implementation of such standards as well as the institutional mechanism for e-governance standards formulation.

> **Example:** The Beckn protocol which is a set of open interoperable specifications, allows buyers and sellers to execute commercial transactions using any platform of their choice. Beckn has enabled a number of initiatives including the Kochi Open Mobility Network (KOMN) and Open Network for Digital Commerce.

1.e. Open APIs: Use publicly available interfaces that allow other developers, programs and services to access data and functionalities provided, and to promote software interoperability for all e-Governance applications and systems. Upcoming digital ecosystems that use open APIs shall adhere to MeitY's National Cyber Security Policy.

Additionally, the specifications on Open APIs published by global organizations like OAS Initiative (Open API Specification) may be adopted as needed.

Example: eSign is an online electronic signature service that can facilitate an Aadhaar holder to digitally sign a document. An Aadhaar holder can sign a document after Biometric/One Time Password authentication thus eliminating the need for paper based application form or documents. eSign makes the process of signing a document digitally very simple and end-users may adopt it at much faster pace than the traditional DSC. The integration is enabled by Open APIs that allow online service providers to easily integrate the eSign facility.[5]

1.f. Open Data: Government departments must proactively open up non-sensitive datasets in formats that facilitate anyone to use, reuse and redistribute it on MeitY's Open Government Data Platform and the National Data & Analytics Platform (NDAP). Open data should be free from any license or any other mechanism of control. This would enhance transparency and accountability while encouraging public engagement.

Upcoming digital ecosystems may also refer to the World Bank Group's Open Data Toolkit for guidance on establishing open data strategies. The toolkit features general standards for data quality, technology options for developing open data platforms, list of open data licenses etc.

International Precedents

1. The United Kingdom's National Digital Twin (NDT) initiative seeks to build a digital representation of assets, processes or systems embracing openness as a fundamental design principle. According to the Gemini Principles that form the backbone of this initiative, NDT must be based on open standards, industry best practices and open application programming interfaces (API) to allow a vendor-neutral approach with industry-agreed architecture models.

2. The US 18F is a Technology Transformation Services office within the General Services Administration (GSA) that collaborates with other agencies to fix technical problems, build products, and improve how the government serves the public through technology. It follows a robust open-source policy and has produced more than 1200+ reusable & interoperable open-source repositories to build effective, user-centric digital services focused on the interaction between the US government and people. A notable project includes DAWSON a case management system, entirely web-based and open source that helps deliver support to resolve tax disputes.

Principle 2: Make unbundled, federated & extendable

Digital ecosystems must follow the unbundled/ building blocks approach where each block has minimal functionality that allows for it to be used in different contexts, thereby leading to time and cost savings. Unbundling when coupled with federation prevents centralization and can increase platform resilience as vulnerabilities are spread out across a 'network of digital building blocks', which ensures that the overall platform can adapt to unexpected challenges without significant disruptions.

[5] https://www.egov-nsdl.co.in/e-sign.html

In this regard, upcoming digital ecosystems must seek to adopt and conform to the enterprise architectural patterns and reference models[6] of IndEA 2.0.

The Gemini Principles by the Centre for Digital Built Britain, the Australian Digital Transformation Strategy and Singapore's Digital Government Blueprint should also be referred to understand how 'building blocks' may be designed and implemented.

Sub-Principles:

2.a. Unbundled: Use a modular architectural framework that makes use of distinct building blocks that can be linked up with each other to offer services.

2.b. Extensible: Design building blocks such that each block has minimal functionality, allowing for it to be combined with other blocks and repurposed in diverse contexts.

2.c. Federated architecture: Employ a structure wherein independent but interconnected systems are loosely coupled to share and exchange information, rather than a single source storing information on all variables. Such a structure guards against the concentration of vulnerabilities at a single point and also ensures the ability to retain federated data ownership and apply the necessary safeguards on data sharing and exchange, such as access control. As highlighted by the IndEA 2.0 framework, these principles must apply to databases, applications, identities and reference data, and to architectural and IT governance.

In this regard, IndEA 2.0 also proposes the setting up of a federated set of registries, linking different digital IDs through open APIs. These federated registries seek to optimize the number of digital identities a user needs to have and simplify the process of authentication. At the moment, publicly-funded schemes, central ministries and States create several identities for the same citizen acting in different capacities. Having multitude IDs to interact with the government increases complexity for the common man and can lead to exclusion of users who are not digitally savvy. In this context, IndEA 2.0 recommends that even as different IDs are being created, users should be given the option to authenticate themselves through any ID they are most comfortable using. This can be enabled in a privacy-preserving and user-controlled manner, by linking ID registries through open APIs. Such a system can facilitate a single sign-ins for people (if they wish to do so) while eliminating repeated verification that is costly, error prone and inconvenient.

> **Example:** India's health digital ecosystem, the Ayushman Bharat Digital Mission follows a federated architectural pattern to safeguard different types of health data while ensuring its interoperability across the ecosystem. Under this, the responsibility of developing building blocks (health IDs, health information exchange, consent manager and health professionals/facility registries) and maintaining different types of health data is shared between centre, state and local facilities.

[6] Refer to Annexure 4, InDEA 2.0

International Precedent: Estonia uses X Road - a centrally managed distributed data exchange system that allows sharing of information in a confidential, secure and interoperable manner. It has also been developed into a tool that can write to multiple information systems, transmit large data sets and perform searches across several information systems simultaneously. To ensure secure transfers, all outgoing data is digitally signed and encrypted, and all incoming data is authenticated and logged.

Two X-road ecosystems can also be federated together to ensure access to data and information. Federation between Estonia and Finland was established in February 2018 to enable easy and secure cross-border data exchange.

Principle 3: Be scalable and nationally Portable

Digital ecosystems must keep their platform design elastic and flexible to accommodate any unexpected increase in demand in the number of transactions, users and other players. While platforms must factor in requirements of localization and diversity, inclusion, and special needs, they should also be designed to ensure national portability to ensure continued access for users even as they move between locations within the country.

A key recommendation for upcoming digital ecosystems to operate at intended scale would also be to adopt cloud-computing[7]. Cloud infrastructure should be chosen as the default, and deployment of applications onsite should be resorted to only with strong justification. This will help reduce local hardware procurement and maintenance requirements. In this regard, adherence to MeitY's Cloud-First Strategy, under which all departments are required to assess and adopt cloud computing for their current as well as new applications, is recommended. To enhance the adoption of cloud technology, MeitY has also empanelled some private Cloud Service Providers (CSPs) that may be leveraged.

> **Example:** Aadhaar's architectural flexibility and national portability has allowed it to scale rapidly. Since its launch in 2009, Aadhaar has seen 1.31 billion enrolments as of October 2021 and the Aadhaar Authentication service is built to handle 100 million authentications a day.

International Precedent: The Ministry of Education in the People's Republic of China developed a national cloud-based education platform that allowed students to continue their studies during the COVID-19 lockdowns. Two months after its launch in February 2020, 270 million students had accessed online classes via the platform. There are numerous similar home-grown examples within India, but this use-case serves as yet another reminder of the benefits of deploying a strategy that allows scalability and portability.

[7] Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud").

Principle 4: Ensure privacy and security

Digital ecosystems must seek to harness data to create public value while ensuring that privacy is protected for users, and security is maintained on the platform. For a digital ecosystem, applying 'security-by-design' and 'privacy-by-design' principles at all the stages of the development of a digital platform - from design to data collection, storage, processing and data sharing is important. This will ensure the safe sharing, use and storage of data across systems and applications both within and across upcoming digital ecosystems.

To maintain platform security, upcoming digital ecosystems must design and enforce an ISMS (Information Security Management System) that conforms to ISO standards for information security. Upcoming digital ecosystems that use open APIs should also adhere to MeitY's National Cyber Security Policy. To ensure privacy, consent mechanisms should also be designed such that consent is freely given, is specific, informed, unambiguous and revocable to give users a genuine choice and ongoing control over their data. This will enhance the reliability of the data and build transparency and trust in the platform. Consent, per the Data Protection Bill under consideration by Parliament, should also be the legal ground for data processing.

Sub-Principles:

4.a. Data security: Use safeguards such as access control, encryption, anonymization etc. to ensure safety of data. The safeguards should adhere to relevant ISO/BIS data security standards such as IS/ISO/IEC 27001 and relevant sections of the Data Protection Bill.

4.b. Data minimization and purpose specification: Collect the least amount of data that may be required for a particular purpose. As far as possible, avoid collecting personally identifiable information.

4.c. Use, disclosure and retention limitation: Offer full disclosure, use data only for the purpose(s) specified, and store personal data for only as long as required.

4.d. Consent: Design consent mechanisms to follow the relevant data protection laws and ensure that consent is freely given, specific, informed and an unambiguous indication of the data subject's wishes. Relevant stakeholders must take it upon themselves to also educate users on the concept of consent in the digital economy.

As highlighted by the General Data Protection Regulation (GDPR), and Section 7 of the 2019 version of the Personal Data Protection Bill, some conditions for consent should be:

> **D1. Free:** The consent is given on a voluntary basis with no direct/indirect pressure on the subject giving the consent.
>
> **D2. Informed and specific**: The subject is notified of the data controller's identity, what kind of data will be processed, how it will be used and the specific purpose for

which it is being collected, as a safeguard against 'function creep'.[8] The data subject is also informed about their right to withdraw consent at any time.

D3. Easy to withdraw: Withdrawal must be as easy as giving consent.

D4. Unambiguous: Consent requires either a statement or a clear affirmative act. Consent isn't implied and is given through an opt-in, a declaration or an active motion, so that there is no misunderstanding that the data subject has consented to the particular ask.

In this regard, the Electronic Consent Framework published by MeitY may be adopted by upcoming digital ecosystems.

Example: The Ayushman Bharat Digital Mission (ABDM) is an example of an ecosystem that aims to incorporate the 'Security and Privacy by Design' principles for the protection of the individual's personal health privacy. It adopts nine principles to govern the use, collection, and processing of personal and sensitive personal data of the data principal viz. accountability, transparency, choice & consent, privacy by design, use and storage limitation, purpose limitation, minimum disclosures & security safeguards under the data privacy policy of ABDM.

International Precedent: The Estonian Government has incorporated 'privacy by design principles' into its e-Estonia ecosystem to safeguard citizens from unauthorised access and misuse of their data. It seeks to obtain granular consent from citizens for each ask, while not maintaining a centralised database and storing the data about taxes, education, healthcare etc. in separate databases. Citizens are also able to decide which entity gets to see what information.

An example of this structure is Estonia's e-health system which is underpinned by Electronic Health Records, a nationwide database consolidated across different healthcare providers. Citizens can access their data by using their digital ID secured using multi-factor authentication (digital certificates and PIN). Other players such as health care providers, pharmacists and insurance providers etc. can only access the data with the citizen's knowledge and consent. The citizen has complete ownership over their data and can allow as well as restrict access to whoever they desire.

The table below presents a quick snapshot of what the privacy-by-design and security-by-design principles mean in practice[9].

[8] 'Function creep' occurs when information is used for a purpose that is not the original specified.
[9] Building India's digital highways: The potential of open digital ecosystems; Omidyar Network India and BCG; Exhibit 5.2, page 54. https://opendigitalecosystems.net/pdf/ODE-Report.pdf

Activity/ Stage	Privacy-by-Design	Security-by-Design
Pre-Operationalising	• Conduct privacy impact assessment before any registry is deployed	• Adhere to International Organization for Standardization (ISO) data protection standard
Data Sourcing	• Seek opt-out consent from individuals; threshold for opt-in • Follow collection limitation – collect what is necessary	• Set minimum privacy and security standards for contributing databases • Use tokenization i.e., unique ID for each database
Storage and Processing	• Use federated architecture – aggregated / anonymized data in central hub; rest of the data should be in silos • Follow purpose limitation – use for what individual has consented to	• Encrypt all data at rest and during transmission • Data breach notification to both regulator and data principals
Data Sharing	• Create personal data stores through API-based system • Follow storage limitation – delete what is not necessary	• Machine-readable policies that stick to data • Department-to-department data sharing based on auditable electronic queries

Principle 5: Develop minimal and evolvable solutions

Digital ecosystems must advocate for iterative and incremental development consisting of adaptive planning, evolutionary development, early delivery, and continuous improvement by encouraging rapid and flexible response to change of all kinds. A recommended way of building evolvable solutions is starting with Minimum Viable Products (MVPs)[10] to which additional features can be added in response to new use cases and understanding of user behaviour.

To facilitate this, upcoming digital ecosystems may adopt a building-blocks approach, where blocks can be classified as core, common or reference based on the degree of decentralisation. As highlighted by the IndEA 2.0 framework, these building blocks can evolve 'orthogonally', such that a change in one building block does not require consequential changes to be made to the other building blocks.

[10] MVP is a product development technique in which a base product is designed with just enough features for early users. Further customization is completed after user-testing and feedback.

Example: Under India's education digital ecosystem – National Digital Education Architecture (NDEAR), core services (IDs, registries, education data exchange, consent manager) are being envisaged as minimal, atomic, and generalized, that will allow builders to "reuse and extend" them to build contextual solutions.

International Precedent: Singapore's Digital Transformation Agency, GovTech Singapore adopts an agile and collaborative approach for all its applications and services to iterate and test solutions. For example, MyCareersFuture.sg, Singapore's job marketplace, was initially launched as a Minimum Viable Product (MVP) version, then beta-tested at career service centres before being developed and launched as a complete product. The agile methodology requires a complete change in working, including sprint (short bursts) planning, continuous engagement between the business and technology functions, and a 'fail fast' culture.

Principles for Driving Community Engagement

Principle 6: Ensure Universal Access

Digital ecosystems must ensure that their digital platforms are 'inclusive by design', i.e., must be designed and developed in a way that caters to the diverse requirements of the intended user base. Special focus must be laid on including populations residing in remote areas and for disadvantaged social groups, to ensure that adoption of digital technologies does not increase barriers to inclusion.

For this, upcoming digital platforms must adhere to MeitY's Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices, Framework for Mobile Governance and Guidelines for Indian Government Websites, to the extent possible.

Building on some of the above provisions, some broad principles that can be operationalised are as follows:

Sub-Principles:

6.a. User-friendly UI / UX: Design a user interface that is easy to access and navigate. Aim for a minimalistic, human-centred, aesthetic design, with easy and smooth navigation, and readily available customer support.

6.b. Vernacular: Ensure that the end-user application is available in vernacular languages. Aim to cover all major Indian languages.

6.c. Accessible Design: Design the end-user application such that it is accessible to people with disabilities and those who can't read. Some potential tools for this could include 'text-to-speech' converters, QR codes etc.

6.d. Omni-channel access through tech: Make services accessible through multiple tech channels (mobile, web, Interactive Voice Response System [IVRS], etc.) to accommodate all levels of technological know-how.

6.e. Omni-channel access through offline mediums: Make services accessible through offline channels such as common service centres to enable access for all users.

6.f. Users have rights to avoid denial of services: If a user is otherwise eligible but does not have some of the required paperwork/ ID cards/ accounts, ensure that there are ways for them to still avail the service.

> **Example 1:** The Unique Identification Authority of India (UIDAI) has notified that Section 7 of Aadhaar Act 2016 has clear provisions to avoid exclusion. If a user does not have Aadhaar or if Aadhaar online verification is not successful due to some reason,

the agency or department has to provide the service by using alternative means of identification and recording them in exception registers.

Example 2: The Government e Marketplace (GeM) platform for public procurement has a user-friendly dashboard, available in multiple languages for monitoring supplies and payments. Additionally, GeM has also undertaken a number of offline initiatives to drive inclusion and participation, including regional workshops to on-board local government buyers, structured onboarding kits to ease the process for vendors and buyers, regular program monitoring etc. Upcoming digital platforms must also seek to adhere to similar design and development principles to ensure universal access.

Example 3: The CoWIN also allows for walk-in entries to address the problem of lack of access. While online registration is available and encouraged, beneficiaries can walk-in to vaccination centers where the vaccination team staff can register them.[11]

Example 4: The National Payment Corporation of India (NPCI) made key financial, non-financial and value-added services of Unified Payments Interface (UPI) accessible to non-internet based mobile devices by integrating it with the Unstructured Supplementary Service Data (USSD) Platform, where users can dial *99# from their phones and transact through an interactive menu. *99# service is currently offered by 83 leading banks & all GSM service providers and can be accessed in 13 different languages including Hindi & English.

International Precedent: UK Government's Digital Development Programme includes a specific Digital Inclusion Strategy that covers challenges relating to digital skilling, digital connectivity and digital service accessibility. It talks about various programmes being initiated, including establishing a cross-government digital capability programme, establishing digitalskills.com as a trusted source of information that helps people and organisations go online, using data to measure performance etc. Integrating such a holistic focus on digital inclusion as a central part of the digital ecosystem agenda will be critical to ensuring access and improving outcomes.

Principle 7: Participatory design and end-user engagement

Digital ecosystems must ensure that they follow a participatory design approach that engages all stakeholders, encourages collective-problem solving and develops digital solutions that meet the needs of a diverse user-base. A collaborative approach will also ensure that concerns, if any, are addressed quickly and no potential user is left behind. This will aid wider end-user-adoption.

[11] FAQ 4, https://www.cowin.gov.in/faq

Sub-Principles:

7.a. Participatory Design and Development: Create avenues to involve the community throughout the value chain i.e. in planning, design, building and operations, by way of public consultations on planning documents and policies, beta-testing with user groups etc. on all major initiatives.

> **Example:** For the development of India's health digital ecosystem – the Ayushman Bharat Digital Mission (ABDM) - the National Health Authority (NHA) has recently invited the public to share their viewpoints on key aspects of the ABDM architecture including the Health Facility Registry, Unified Health Interface and Health Data Retention Policy etc. The NHA has also followed a similar consultative approach with most of its policy papers being released for consultation before finalization.

7.b. End-user adoption: Proactively encourage adoption by using means such as awareness campaigns, building reference applications to demonstrate use cases etc. Also provide ongoing support in the form of FAQs, guidelines and usage documentation to facilitate effective use.

The potential of digital platforms to generate new economic value largely depends on the extent of their end-user adoption Therefore, providing instructive guidelines/awareness campaigns that target a particular demographic/vulnerable social group can help in driving adoption.

> **Example 1:** MeitY's DigiDhan Mission was set up to promote the uptake of digital payment systems in the country, and to this end, it organises promotional campaigns, training activities etc. to generate awareness benefits of digital payments.

> **Example 2:** The National Payment Corporation of India (NPCI) developed BHIM as a mobile payment application, based on Unified Payments Interface (UPI) which has served as a reference application for the development of many private mobile payment applications such as PhonePe, Gpay etc.

International Precedent: Singapore's digital transformation agency, GovTech Singapore has created a community of end-users who are allowed to test new technology solutions and provide feedback for improvement, before the services are launched at scale. Upcoming digital ecosystems must seek to deploy such feedback mechanisms from users to ensure that the architecture remains user-centric.

Principle 8: Cultivate a network of innovators

Digital platforms can benefit greatly from innovators and independent technical experts to expand the range of services they offer as well for undertaking modifications/ enhancements to improve service delivery. As highlighted by the IndEA 2.0 framework, the focus must be to 'enable rather than build' i.e., the aim of the ecosystem approach fundamentally relies on

adoption by innovators who can take advantage of the shared-technology infrastructure to build services on top.

Sub-Principles:

8.a. Proactively engage with tech experts to build the base infrastructure layer: Provide mechanisms for experts to contribute to the development process and enable improvements in the platform's performance through bug bounty programs etc.

> **Example 1**: The Advisory Council for Open Network for Digital Commerce (ONDC) includes several technical experts both from within the government as well as from the industry to guide the design and development of ONDC. Similar engagements must be undertaken for upcoming digital ecosystems.
>
> **Example 2:** After the source code for the Aarogya Setu application was released, a bug bounty program was also launched by the government to identify vulnerabilities and suggest improvements to the source code.

8.b. Proactively engage with innovators to build solutions on top of the base infrastructure layer: Enable innovation, and responsible deployment of emerging technologies by supporting the development of new solutions through mechanisms such as sandbox testing, incentive-based innovation challenges/ hackathons, incubation centres and other test beds.

> **Example 1:** The Ayushman Bharat Digital Mission (ABDM) has outlined guidelines for sandbox testing which will allow innovators to test their products or services in a controlled environment. Upcoming digital ecosystems must also seek to provide such a structured mechanism for engaging with innovators, which helps facilitate consumer-centric and responsible innovation. The NHA, in collaboration with the Indian Software Products Industry Round Table (iSPIRT), has also conducted innovation challenges like Healthathon 2020 that encouraged innovators to come up with business plans and product ideas around the Personal Health Record (PHR) system.
>
> **Example 2:** The India Urban Data Exchange (IUDX) platform aims to open public data (such as traffic patterns, street lighting and sensors, land use, crime, etc.), to innovators to build new solutions in the context of urban governance such as for smart mobility, women's safety, etc. In doing so, the platform provides innovators with the core technology infrastructure and technical specifications required for integration, but does not necessarily create end-user solutions. The success of this platform and its impact on urban lives will, therefore, depend on its adoption by innovators who can take advantage of the infrastructure to build services on top of it.

IUDX is currently creating an IUDX consortium, which will make it easy for all types of companies – including public, private entities as well as start-ups - to work with IUDX and the cities deploying IUDX.[12]

International Precedent: Open Data DK provides a framework for knowledge sharing about open data between public authorities and businesses across Denmark. To ensure wider participation from the community of innovators, Open Data DK regularly undertakes a range of activities including hackathons, informal meetups and connection sessions with coders, academics etc.

Principle 9: Be analytics-driven and service-oriented

Digital platforms must deploy mechanisms to systematically collect feedback from end-users to gauge adoption barriers, improve platform performance, design new solutions, formulate evidence-based policies etc. Additionally, platforms must be value-driven and outcome-oriented, and should follow standard practices for uniformity and consistency in service delivery.

To this end, upcoming digital ecosystems may adopt the methods outlined in MeitY's Digital Service Standard (DSS). This document suggests a set of inter-related standards that can apply to all aspects of a digital service, through its lifecycle. It also provides a framework to measure the performance of digital services and to assess their impact, while also presenting a set of strategies to overcome challenges. Finally, it recommends that digital services may follow a 'Whole of Government' approach, where all the departments and agencies of the government should endeavour to move towards a connected government.

Sub-Principles:

9.a. Analytics-driven for continuous user-focus: Employ data analytics tools that track the number of active users, number of downloads etc. to evaluate the extent of end-user adoption. This data can then be used in conjunction with other user experience research methods to improve accessibility and user-centricity of services.

9.b. Service oriented: Ensure that service delivery focusses on providing additional or new value to the user. Define and measure service levels, impact and outcomes to ensure service delivery is outcome-driven.

Example: Most digital platforms that have been developed in the recent past in India leverage analytics to measure uptake and quality of service delivery. The CoWIN platform is one example of such a system that is analytics driven. In the case of CoWIN, feedback from users has also been critical for improving vaccination delivery through this platform. Such practices need to be systematically imbibed and incorporated in all upcoming digital applications and ecosystems.

[12] https://iudx.org.in/partnerships/

Principle 10: Enable Responsive Grievance Redressal

Providing robust grievance redressal mechanisms will enhance user experience and build accountability and trust in the platform. Guidelines for grievance redressal should include those that are related to the functioning and operation of the platform, as well as ones that relate to the quality of services provided. Such systems will be critical for driving user adoption.

Sub-Principles:

10.a. Set up a responsive grievance redressal system: Provide for grievance redressal with clear offline and online escalation procedures published through a service charter for different types of grievances along with commitments on time required for issue resolution, as well as procedures for appeal. It is particularly important to augment online touchpoints and processes with a human point of contact, especially for ensuring last-mile access.[13] This can be accomplished by local government representatives or civil society organisations, including non-profits.

Where possible, establish a legally backed redressal mechanism will ensure that intended users of the platform have the right to secure proper and timely delivery of services and benefits.

> **Example:** DIGIT is an open source urban governance platform that includes a Public Grievance Redressal module which incorporates a variety of touchpoints, including a call center, mobile app, web portal, and email for individuals to register grievances. Upcoming digital ecosystems must also seek to provide similar multi-channel grievance redressal mechanisms to enhance the experience of the end-user and ensure accountability of the platform.

[13] Aapti Institute. Last Mile Access Study. https://uploads.strikinglycdn.com/files/294143ba-333f-4bcc-9379-6d4742d15509/Last%20Mile%20Report-Digital-Aapti%20Institute.pdf

Principles for Strengthening Governance

Principle 11: Define Accountable Institutions

Digital ecosystems must adhere to the principles of open, transparent, participatory governance and appropriate accountability frameworks must always be maintained. Assigning responsibility to a specific institution is also essential to ensure ownership; this can help drive the development of the ecosystem as well as its adoption by users.

As a first step, this involves identifying an accountable institution for each digital platform, whether a public entity or a coalition set up as a Special Purpose Vehicle (SPV) or a Public-Private Partnership (PPP), that is responsible for the overall administration of the platform and setting the standards and rules of engagement that drive accountability.

Accountable institutions must be holistic in nature with the right legal and organizational structure, and operating processes that are aligned with platform objectives. It is also imperative that such institutions work closely with the sectoral regulators.

Sub-Principles:

11.a. Designate an accountable institution: Designate an institution that is responsible for the overall management of the digital platform, including strategic and financial decision-making, driving builder and end-user adoption, and creating policies for stakeholder engagement.

> **Example 1:** The National Urban Innovation Hub (NUIH) has been identified as the foundational institution that will identify, partner and coordinate with various stakeholders across the ecosystem to drive the development of the urban digital ecosystem.
>
> **Example 2:** The Open Network for Digital Commerce (ONDC) has been set up as a Section 8 company under the Companies Act 2013,[14] to oversee the development of India's first-ever open network for exchange of goods and services online. It is expected to empower consumers and sellers by allowing them to connect online outside of closed-loop platforms.
>
> **Example 3:** The National Payments Corporation of India (NPCI), an umbrella organisation for operating retail payments and settlement systems in India, is an initiative of Reserve Bank of India (RBI) and Indian Banks' Association (IBA) under the provisions of the Payment and Settlement Systems Act, 2007, for creating a robust payment and settlement infrastructure in India. As the accountable institution for payments, NPCI prescribes rules, regulations, guidelines, and the respective roles, responsibilities and liabilities of market participants. This also includes transaction processing and settlement, dispute management and clearing cut-offs for settlement.

[14] https://twitter.com/ondc_official/status/1477504761683275777

Upcoming digital ecosystems must also seek to establish similar accountable institutions that will oversee the delivery of different solutions by various stakeholders in the ecosystem. Such institutions will also be able to provide the technical expertise needed for the management of the platform.

11.b. Maintain government oversight: The accountable institution can either be a public entity, or a public private partnership, or a not-for-profit entity such as a Section 8 company with strong government oversight. Government oversight is critical because (1) the accountable institution is tasked with developing and maintaining the core digital infrastructure around which the rest of the ecosystem is anchored; and (2) the policies created by the institution determine access to innovators and other community players through rules of engagement. To ensure that there is no private capture and that public interest remains central to decision-making, government oversight becomes essential.

The institution should ideally also be accountable directly to the general public, either by virtue of being covered under the RTI Act or through another mechanism specific to the institution.

> **Example 1:** The National Health Authority (NHA) has been identified as the institution that is entrusted with managing day-to-day operations, developing strategic partnerships with private and civil society organisations, coordinating between various ministries and departments for the implementation of the Ayushman Bharat Digital Mission (ABDM). It was set up through a 2019 gazette notification[15], that created the NHA as an attached office of the Ministry of Health and Family Welfare with full functional autonomy. The NHA is governed by a Governing Board comprising of a Chairman and 11 members, with the Chairman being the Union Minister for Health and Family Welfare, GOI. It is also covered under the RTI Act.[16]

11.c. Multi-Stakeholder engagement in governance: Set up an organizational structure that promotes the involvement of different stakeholders in governance processes through independent advisory groups, consumer ombudsman etc. Multi-stakeholder governance that fosters greater collaboration between actors in the ecosystem, drives greater trust and transparency.

> **Example 1:** The National Health Authority (NHA) has laid out guidelines for engaging the services of stakeholders, as independent volunteers who can advise the formulation of policy and guide the development of Ayushman Bharat Digital Mission (ABDM).

International Precedent: The RIA of Estonia is the institution under the Ministry for Economic Affairs and Communications (MEAC) for developing and managing the X-Road ecosystem. It registers new members, documents data exchange between members, and supervises the security of the information systems. Specifically, it plays the role of a watchdog,

[15] https://pmjay.gov.in/sites/default/files/2020-01/E-Gazette_of_NITI_creating_NHA.pdf
[16] https://pmjay.gov.in/rti

i.e., it collects statistical information about data transfer through X-Road to oversee the ecosystem and manage any risks that may arise. This model separates the strategy and implementation roles, establishing accountability while housing both departments under the same ministry to facilitate coordination.

Principle 12: Establish and align robust rules of engagement

To ensure a level playing field in a multi-stakeholder system, establishing rules of engagement that outline the manner in which different stakeholders[17] can engage with the platform, including eligibility criteria, rights of access, roles and responsibilities will help broaden participation, spur innovation and also avoid mismanagement and conflicts of interest.

The terms of engagement should be outlined through publicly available standard norms/ MoUs that apply uniformly to all stakeholders. This can help prevent preferential treatment/unfair value capture.

> **Example:** The Unified Payments Interface (UPI) ecosystem is comprised of multiple stakeholders including banks and PSPs. The roles and responsibilities, including liabilities of all stakeholders such as for user data protection, have been clearly laid out by NPCI under Procedural Guidelines for UPI. These guidelines have been framed under the provisions of the Payment and Settlement System Act, 2007 and are binding on all members of the UPI ecosystem. For instance, new guidelines issued limits the share of digital payment applications in the overall volume of transactions on the unified payment interface at 30% to ensure a level playing field.[18]

Principle 13: Create transparent data governance

In a digital ecosystem, interoperability allows data silos to be broken down to create shared technology infrastructure that allows for data to be exchanged more freely between information systems. This raises the risk of data misuses and data breaches (especially of sensitive, personal data) and therefore a robust data governance framework that defines institutions, legal and regulatory policies, and processes is necessary. Data policies and standards on ownership, collection, contribution, consumption of data (especially sensitive personal data) that establish non-repudiability[19] must be established, and adhered to by all upcoming digital ecosystems. This will bring transparency while ensuring that the integrity of the data is preserved.

[17] Stakeholders may include other government departments that seek data/ leverage services, innovators, civil society actors, end-users including businesses and individuals etc.
[18] NPCI. Standard Operating Procedure (SOP) – Market Share Cap for Third Party Application Providers (TPAP). https://www.npci.org.in/PDF/npci/upi/circular/2021/standard-operating-procedure-sop%E2%80%93market-share-cap-for-third-party-application-providers-tpap.pdf
[19] Non-repudiation refers to the ability to prove that data has not been altered

Sub-Principles:

13.a. Easy-to-understand: Ensure that policies on data are presented in a simple-to-understand manner and not in dense legalese and can be readily found by users.

13.b. Adopt mechanisms to create audit trails and ensure data validity: Each data item should be accompanied by a record of its complete journey, that is, original source, frequency and details of any subsequent modifications, details of modifiers, and any other individuals or entities that might have handled the data. Maintaining such records will ensure the auditability, transparency, and reliability of the digital platform.

13.c. Drive adherence: Deploy robust mechanisms and clearly identify liability to monitor and drive adherence on data governance.

13.d. Ensure end-user ownership: Provide end-user ownership through mechanisms for users to correct, complete, and update misleading, incorrect, and out-of-date personal data. Mechanisms should also operationalize the right to be forgotten.

While some data points (birth date, place etc.) remain constant over time, other data points relating to demographic information (such as address, education, employment, health status etc.) of an individual can change over time. Without a provision for correcting/ updating this information, citizens run the risk of being mistargeted/excluded. Given the large informal sector and migrant labour force in India, information regarding household situations changes quickly, and sometimes unpredictably. Therefore, provisions for end-user ownership and control over data are especially important for driving inclusion.

> **Example:** Recognizing these challenges, UIDAI has created provisions to allow users to change/correct demographic details, including name, gender, address etc. A card holder can submit relevant documents to request a change, either online through Aadhaar's self-service portal or offline by visiting a permanent enrolment centre.[20]

International Precedent: The Estonian Data Protection Inspectorate, is the national Data Protection Authority for Estonia, in charge of enforcing GDPR in the country. The Inspectorate's mandate is to protect the rights to obtain information, and the right to inviolability of private and family life in the use of personal data. It does so through various legal and institutional mechanisms. For instance, to promote usage specification that allows only minimum data collection and sharing, it levies heavy penalties in cases of unauthorized access to data. Be enforcing provisions under domain specific laws such as the Medicinal Products Act, it allows individuals to prohibit any healthcare provider from accessing their personal data stored in the Digital Prescription Centre. It also enforces statutes which specify the procedure for maintenance of the database, including the chief processor. Additionally, individuals are also provided access to a Personal Data Usage Monitor, an AI-enabled software

[20] https://uidai.gov.in/my-aadhaar/about-your-aadhaar/updating-data-on-aadhaar.html

that allows them to view logs of all instances of their personal data being used by the government.

To create transparency around upcoming digital ecosystem designing similar legal and institutional mechanisms must be explored.

Principle 14: Ensure the right capabilities

The development of a digital ecosystem requires specialised expertise in core areas such as enterprise architecture, data analytics, cybersecurity, design thinking and user support. Upcoming digital ecosystems should therefore ensure that they have access to the requisite talent to provide these capabilities.

Sub-Principles:

14.a. Talent management: Ensure the right capabilities by setting up systems for developing in-house talent through capacity building. Additionally, provide the ability to hire and retain top-quality, fit-for purpose tech and non-tech talent through effective, nimble strategies.

The IndEA 2.0 draft stresses on the need for capacity building, especially since there is significant detailing to be done in the context of any Ministry or State to create the right architecture and building blocks. It proposes systematic programs to create capacities and competencies on design and implementation in both public and private organizations, especially among two target groups - government staff including policy makers and administrators at the centre and states (such as secretaries and heads of department) and professionals including CTOs, COOs, architects, system analysts, CISOs and privacy officers. The IndEA 2.0 draft also goes into some depth in prescribing the kinds of themes and modules that may be needed (see Chapter 7, IndEA 2.0 framework)

> **Example:** UIDAI, the statutory authority responsible for managing Aadhaar, has a unique talent acquisition strategy where it enlists the services of experts from academia and industry from relevant backgrounds to work with UIDAI. It lays down the recruitment guidelines for professionals, volunteers and sabbatical/secondment officers and details out the manner of engagement, selection criteria and the code of conduct.
>
> Upcoming digital ecosystems must aim to establish similar talent acquisition models that bring in cross-domain expertise to government projects.

14.b. Agile Procurement Policies: Ensure the right capabilities by designing appropriate procurement policies that allow for the selection of top-quality partners/ external agencies/ vendors. Leverage agile procurement to acquire solutions according to the desired outcomes, rather than by prescribing a set of detailed requirements and specifications.

This principle builds on the understanding that requirements are usually too high-level and coarse at the conceptualization stage of a project and often evolve rapidly as the project progresses. Therefore, it is difficult to create specification level bid documents that help bidders understand the scope of the project, and establish a level playing field.

To address this challenge, procurement policies should be designed keeping the following recommendations in mind:

- The focus should not be on buying software, but jointly designing and building a new and innovative system.
- Incremental pricing should be preferred to the traditional fixed-price arrangements. This could mean using pay-per-use model of IT infrastructure (by using cloud services) and pay-per-transaction model (for each service delivered).
- The focus should also change from contract management to performance management in the post-award period.

See section 3.7 in Agile IndEA for more details. MeitY's Guidelines for Procurement of Cloud Services may also be useful in this regard.

Example 1: The Goods and Services Tax Network (GSTN) platform leverages a network of partners that provide expert capabilities and services for maintenance and service delivery. For instance, Infosys has been engaged for building and maintaining the software, Wipro manages the TINXSYS - a centralized exchange of all interstate dealers - supporting verification and reporting, and Tech Mahindra supports the GSTN help desk.

Example 2: An example of a project that has been implemented on a pay-per-transaction model is the Passport Seva project[21] that was launched in 2010 to improve the delivery of passport services to Indian citizens. The project has been implemented in a Public Private Partnership (PPP) mode with Tata Consultancy Services, selected through a public competitive procurement process.[22]

Upcoming digital ecosystems may also engage the services of domain experts from the private sector to guide the development and manage the operation of their respective platforms.

International Precedent 1: Singapore's digital transformation agency, GovTech Singapore has introduced several innovative contracts to streamline its information and communication technology (ICT) procurement processes. An example of such an initiative is 'Spiral Contracting', which comprises multi-stage contracts. In this case, contracts will be written with multiple stages, with the project progressing to subsequent phases of prototyping, piloting and deployment only if the first phase is successful. Another example is 'Dynamic Contracting' (for bulk tenders), that allows for the addition of either new requirements or new vendors (suppliers), at any point in the contract.

[21] Example cited from Agile IndEA, page 18
[22] https://www.passportindia.gov.in/AppOnlineProject/online/knowPassportSeva

International Precedent 2: Australia's Digital Transformation Agency has instituted a 'Digital Sourcing Lifecycle' process that consists of three phases – 'plan', 'source' and 'manage'. Each of these phases includes a set of recommended tasks and a range of tools that further eases the ICT procurement process.

Principle 15: Adopt a sustainable funding model

In order to maximise the impact of digital ecosystems, a financially viable, sustainable funding model is crucial. This can enable smooth functioning as well as future improvements and innovation. At different stages of the life cycle of a digital ecosystem, different financing models may be also required.

In a recent paper published by the Data Governance Network - Financing Models for Digital Ecosystems – the authors analyse the suitability of government, market and philanthropic financing to each component of the digital ecosystem, keeping in mind both market and non-market failures.

Sub-Principles:

15.a. Allocate sufficient funding for initial design and development: Earmark adequate funding in the government budget, or through other sources, for the initial design and development phase of the platform.

> **Example:** The budgetary allocation for Ayushman Bharat Digital Mission (ABDM) in 2021-22 was ₹30 crore. And this has been increased to Rs. 200 crore for 2022-23 as the scope of operations has expanded. These resources are expected to lay a sound foundation for the base digital infrastructure on which other services may be developed by innovators.

15.b. Adopt a sustainable business model for operations and maintenance (O&M): Explore mechanisms to generate revenue through service charges, subscription fee or otherwise to support the upkeep of the platform. Alternatively, ensure that O&M expenses are supported through recurring line items in the government budget.

> **Example 1:** The Unique Identification Authority of India (UIDAI) which is the statutory body responsible for Aadhaar enrolment and authentication, also charges for some Aadhaar-related services such as biometric or demographic updates, printing of the e-Aadhaar card etc. that go towards the upkeep of the platform. This revenue stream supplements the budgetary support that it gets through the government.

15.c. Diversified pool of funders: If the plan is to leverage donor funding, ensure that there is no dependence on a single donor, and dependence – if any - is time-bound. This will help hedge future risks to funding, while guarding against the potential of unfair value capture by a private player.

Example 1: DHIS2, an open source, web-based platform most commonly used as a health management information system (HMIS) has been developed, maintained, and implemented by leveraging funding from different kinds of institutions including, philanthropic foundations, multilateral institutions and bilateral aid agencies. Some funders of DHIS2 include the Bill and Melinda Gates Foundation (BMGF), the World Health Organisation (WHO), UNICEF, Norwegian Agency for Development Cooperation (NORAD) etc.

Example 2: MOSIP, a modular and open source identity platform that helps Governments implement a digital foundational ID systems is supported by 3 philanthropic organisations, Bill & Melinda Gates Foundation (BMGF), Sir Ratan Tata Trust and Omidyar Network.

Example 3: Raast, Pakistan's recently launched digital payment system, was developed in collaboration with the State Bank of Pakistan and the Bill & Melinda Gates Foundation. It also received support from the United Kingdom, the United Nations and the World Bank.

Way Forward

The world is at the cusp of a digital revolution. As we make the shift towards the new 'ecosystem' form of service delivery, it becomes imperative that the digital ecosystems we co-create are open, inclusive and safe for all. It is with the same objective that this implementation blue book provides avenues for operationalizing key principles of the IndEA and NODE frameworks to design and implement digital ecosystems at scale. In this blue book, we focus on not just the 'tech' aspects but also the very critical 'non-tech' aspects of community engagement and governance.

Both the central government as well as several state governments have realized the potential of the ecosystem approach. At the central level the Aadhaar Stack is a prime example of a successfully built digital ecosystem, whereas state level initiatives include Madhya Pradesh's Samagra, Haryana's SARAL, Telangana's Samagrah Vedika and Andhra Pradesh's e-Pragati, among others. As more states and sectors work on developing or refining their digital infrastructure, this document can help set a standard for existing ecosystems, while providing a direction for the new ones that are being planned or built.

Establishing a Digital Ecosystem Council

As diverse stakeholders engage with the implementation of digital ecosystems, there is a need for a coordinated authority to drive this initiative. To this end, an 'India Digital Ecosystem Council' may be instituted to develop standards, advise on various design and implementation aspects of these ecosystems, and facilitate their large-scale adoption. This Council can comprise of multiple verticals, such as Technology, Data Governance, Ethics, Operations and Community Engagement, to ensure and enforce a holistic oversight mechanism. Each of these verticals may include industry experts and academia, both from public and private sectors, and from diverse fields such as public policy, technology, ethics, product development, data analytics, behavioural sciences etc. Additionally, it can have participation from central ministries and state governments to allow for sectoral and state perspectives. The broad objectives of this council could include:

- Strategizing for the adoption of the digital ecosystem approach both at sectoral and state levels.
- Developing and revising the required policies, guidelines, and frameworks and ensuring consistency across digital ecosystems.
- Advising ministries and states on the design and implementation of digital ecosystems to enable faster decision-making.

The digital ecosystems approach can bring immense benefits by facilitating seamless delivery of welfare benefits across different sectors including education, agriculture, financial inclusion, healthcare, skilling etc. To make this vision a reality, this blue book hopes to provide a framework for practitioners, policymakers and innovators to develop and scale digital ecosystems in an inclusive and sustainable manner.

Case Study
Ayushman Bharat Digital Mission: India's National Open Digital Ecosystem for Healthcare

Note: This is a shortened version of a longer case study on ABDM that has been published separately alongside this implementation blue book.

The Ayushman Bharat Digital Mission (ABDM) is envisioned as an ecosystem that seeks to create a 'holistic, comprehensive and interoperable digital architecture' to 'support Universal Health Coverage in an efficient, accessible, inclusive, affordable, timely and safe manner.'[23] The core idea behind the framework is to allow for seamless and safe exchange of health information among various stakeholders and across the ecosystem, to provide personalized and user-centric health services. Through its implementation it seeks to improve the efficiency, effectiveness, and transparency of health service delivery so as to improve overall health outcomes.

There are 3 key strategy documents that are actioning this agenda - the National Digital Health Blueprint (NDHB) that outlines the core principles and architectural vision of ABDM, the National Health Stack that presents the set of building blocks to be developed, and the ABDM Strategy that presents the implementation framework. Additionally, specific consultation papers, guidelines and policies have also been published to support the evolution of the digital health ecosystem.

In this case study, we highlight how design elements and policy criteria of ABDM, as indicated by the above documents, adopt and align with MeitY's IndEA and NODE Principles.

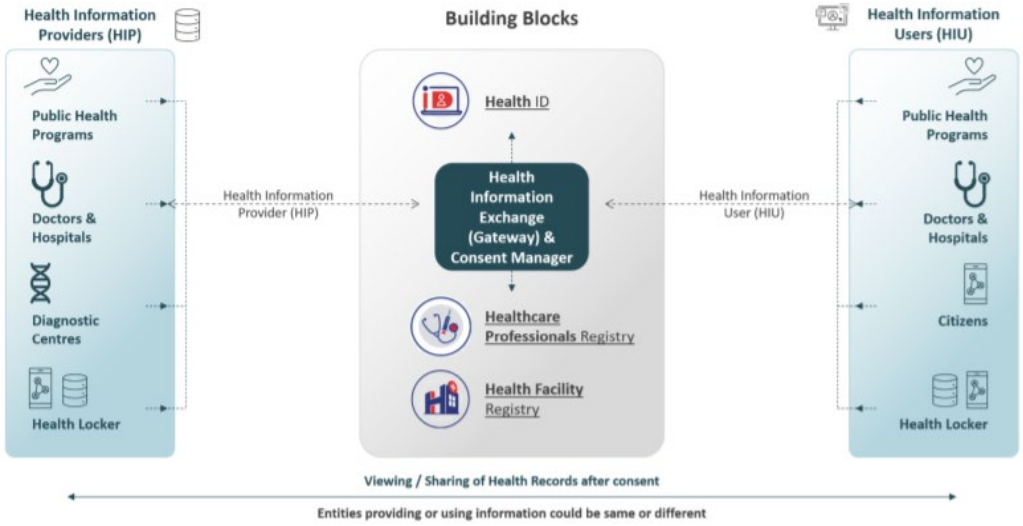
Ayushman Bharat Digital Mission: Mapping against the IndEA & NODE Principles

Technology layer:

Given the enterprise nature of the ABDM framework, its fundamental technology principles and domain principles, by default, adopt and align with the IndEA principles. The blueprint highlights the centrality of Principle 1 i.e., of being open and interoperable by stating that MeitY's Policy on open standards and open-source software and Open APIs will be adopted in designing of the building blocks, which is fundamental for ensuring interoperability. Further, the ABDM Blueprint recommends the gradual adoption of internationally recognised open health standards, in areas where standards have not been prescribed by IndEA. The Unified Health Interface (UHI) that represents the foundational layer of the ABDM infrastructure is also envisioned as an open protocol for various digital health services.[24] Currently, an open source community is developing 'Decentralized Health Protocols (DHP)', which by facilitating interoperability between healthcare providers and users, will enable the provision of digital health services through the UHI Network.

[23] ABDM Strategy Overview https://abdm.gov.in/publications/ndhm_strategy_overview (pg.38)
[24] https://abdm.gov.in/Home/collaborative_development

The technology principles also underscore the importance of adopting a federated architecture (Principle 2) and the need for a minimalist approach (Principle 5) while designing the 'building blocks' that form the National Health Stack (NHS), or the basic infrastructure layer of ABDM. Under this, the responsibility of developing 'core building blocks' (health IDs, health information exchange, consent manager and health professionals/facility registries) and maintaining different types of health data will be shared between centre, state and local facilities. Other building blocks needed at multiple levels will be developed and operated by other players in the ecosystem. By adopting such an architectural pattern, the ABDM framework seeks to safeguard different types of health data while ensuring its interoperability across the ecosystem.



NDHM Building Blocks[25]

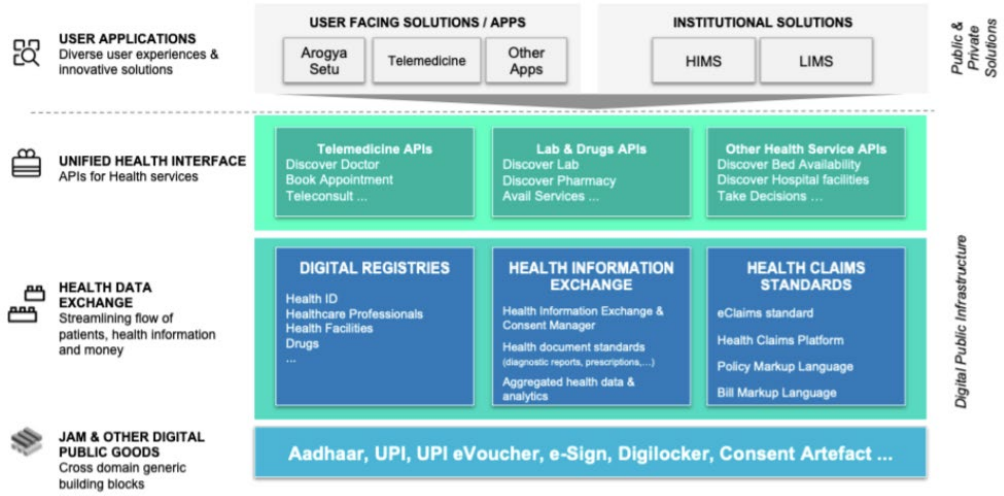
The National Digital Health Blueprint outlines the importance of the ecosystem being inclusive, wellness-driven and one that ensures security and privacy by design. By creating building blocks such as *Consent Manager*, *Anonymizer* and *Privacy Operations Centre*, the ABDM puts in place mechanisms to maintain the confidentiality, security and privacy of health data i.e., operationalizes Principle 4.[26] The *Consent Manager* places the data principal in control of their data; the *Anonymizer* removes personally identifiable information before sharing the data; and the *Privacy Operations Centre* monitors the overall process to enhance trust in the system. While modules such as the anonymization-as-a-service are not yet developed, the Data Protection Bill is expected to set the standards and provide a framework for such anonymization procedures. Further, all building blocks that involve the handling of personal health data will be required to comply with the National Policy on Security of Health Systems and Privacy of Personal Health Records that will be developed[27] to ensure that privacy and security of data is incorporated in these building blocks from the design stage.

[25] https://abdm.gov.in/assets/uploads/consultation_papersDocs/UHI_Consultation_Paper.pdf
[26] Principle 4: Ensure privacy and security
[27] National Digital Health Blueprint, Page 10

In December 2020, the government approved the National Health Data Management Policy that lays down the guiding principles for Security and Privacy by Design under ABDM. It provides detailed guidelines for data minimisation; purpose limitation; collection, use and storage limitation; and informed and free consent for data-sharing. The NHA also recently released a Consultation Paper on Health Data Retention Policy that lays down guidelines for data retention by health facilities and seeks to ensure that data retention guidelines are in sync with all applicable legal and regulatory compliances.

Community layer:

The ABDM framework incorporates several mechanisms to drive inclusion and meaningful adoption, to align with Principle 6 on ensuring universal access. The ABDM building blocks are envisioned to be user-friendly so that users can easily access them to develop and upgrade necessary applications.[28]



UHI Layer in the NDHM architecture[29]

The National Health Authority also plans to develop specialised systems to extend the ABDM framework to those residing in remote areas, with limited digital reach.[30] This includes the usage of omni-channel tech mediums, including mobile phones, call centres and social media platforms to extend services. Given the rapidly expanding smartphone coverage in the country, ABDM also seeks to adopt a 'Mobile First' principle whereby all digital services will be designed such that they can be delivered through smartphones. It also seeks to develop a voice-based service in vernacular languages to overcome language barriers and increase adoption.[31] While these are steps in the right direction to mitigate the exclusion risk, the framework is still at a nascent stage and it remains to be seen how these steps are implemented.

[28] ABDM Strategy Overview https://abdm.gov.in/publications/ndhm_strategy_overview (pg.38)
[29] https://abdm.gov.in/assets/uploads/consultation_papersDocs/UHI_Consultation_Paper.pdf
[30] https://abdm.gov.in/publications/ndhm_strategy_overview (*1.6.2 Guiding Principles)*
[31] ABDM https://abdm.gov.in/home/ndhb (pg 26)

The ABDM also recognizes the importance of engaging with the active builder/developer community to foster innovation, and thereby conforms to Principle 7 on following a participatory design approach and Principle 8 on cultivating a network of innovators. The NHA has been actively engaged on this front. To cite an example, the NHA published a consultation paper on the Unified Health Interface in July 2021 and received extensive feedback (available on its website here) on the technical and functional design elements of UHI. Involving the community in deciding the technical specifications and protocols can go a long way in not only ensuring public scrutiny and enhancing public trust in these systems, but also reduce hiccups at advanced stages of developing or deploying a digital ecosystem.

The NHA, in collaboration with Indian Software Products Industry Round Table (iSPIRT), has also conducted innovation challenges like Healthathon 2020 that encouraged innovators to come up with business plans and product ideas around the Personal Health Record (PHR) system, as well as build those products on top of the PHR system using open APIs. Further, the NHA has been organising webinars and open house discussions to appraise the public of the architecture of ABDM. Similarly, iSPIRT has been regularly promoting content explaining the workings of the ABDM system to increase awareness. ABDM also recognizes the importance of Principle 9 i.e., being analytics-driven and therefore, going forward, plans to focus on beta testing while evaluating adoption and performance before going live for all ABDM components (in the phase three of ABDM).

Finally, the National Digital Health Blueprint sets out a fairly comprehensive mechanism that allows for the appointment of a Data Protection Officer and a Grievance Officer who would be responsible for addressing the complaints put forward by the data principal in a timely and effective manner. Additionally, the Health Data Management Policy outlines that the complaint must be resolved by the Grievance Officer within a period of one month. In doing so, it acknowledges the importance of instituting robust grievance redressal mechanisms to enhance user experience while building accountability and trust (Principle 10).

Governance layer:

In the case of ABDM, there are three institutions, viz. the Ministry of Health and Family Welfare (MoHFW), the Ministry of Electronics and Information Technology (MeitY), and the National Health Authority (NHA) – that are in charge. The Ministries are responsible for defining the legal and regulatory framework of the Mission, and the NHA is primarily tasked with the implementation, which includes managing day-to-day operations, developing strategic partnerships with private and civil society organisations, coordinating between various ministries and departments, etc.

For instance, the NHA recently issued tenders to invite and onboard Managed Service Providers, Managed Cloud Services Providers, etc. It developed strategic partnerships with Swasth Alliance and iSPIRT, which have been onboarded on a volunteer basis in compliance with the Volunteer Guidelines laid down by NHA for technical assistance in building the health data consent manager. It also instituted a dedicated position - Joint Director (Coordination) -

to promote and facilitate coordination between various state governments for effective implementation of ABDM.

As highlighted by Principle 12 (establish and align robust rules of engagement), given that such an ecosystem often has multiple touch points and stakeholders, it becomes imperative that the accountable institution lays down the rules of engagement between various entities. This includes outlining the roles, rights, responsibilities and liabilities of various actors in the ecosystem. In the case of ABDM, the NHA has released several policy documents laying down the rights and responsibilities of the involved stakeholders. Some of these documents include the Health Data Management Policy (HDMP) for Health Information Users and data fiduciaries, Guidelines for Health Information Providers, Health Repository Providers, Health Information Users and Health Lockers for Health Information Users and Health Information Providers, and ABDM Sandbox Guidelines for health tech service providers. In addition to these documents, the ABDM Strategy overview and National Digital Health Blueprint also detail out rules of engagement for data consumers, processors, and citizens. These documents are available on the ABDM website for anyone who wishes to get acquainted with them.

Apart from the aforementioned ABDM-specific guidelines and regulations, there are other existing frameworks such as the Telemedicine Practice Guidelines, E-pharmacy regulations and the Information Technology (IT) Act that extend to ABDM as well. All of these help further the adoption of Principle 13 (creating transparent data governance). A law/regulation that will shape ABDM going forward would be the Data Protection Bill which will, *inter alia*, recognize the right to be forgotten, allowing an individual to withdraw consent at will and retain the control of their personal data.

Finally, the success of a digital ecosystem depends on the funding model and the ability to acquire and retain high quality talent i.e., as highlighted by Principle 14 and 15. In terms of funding, since ABDM is envisioned as Digital Public Infrastructure, it is slated to receive budgetary support from the government in the early years to finance the initial capital and operating costs. The budgetary allocation for ABDM in 2021-22 was ₹30 crore, which is the same as the revised estimates of FY 2020-21. The allocation in 2022-23 was increased to Rs. 200 crore in light of expected expansion of operations.

Going forward, ABDM seeks to co-opt public and private players in building and operationalising other building blocks like Health Exchange, Health IDs, etc. The National Digital Health Blueprint also states that it may raise a part of the funding through a transaction fee, however, this would be on the lines of a toll-pricing model without a profit motive as it could otherwise dilute its 'public good' utility.