Sattva Knowledge Institute SKI primer

SHAPING TRANSFORMATION: POLICY LANDSCAPE OF INDIA'S DIGITAL PUBLIC INFRASTRUCTURE

April 2023

Acknowledgements

Contributors

Shreyanka Chandel, Bhavi Shah, Arnab Mukherjee and **Abhishek Modi.**

Disclaimer

This report has been produced by a team from Sattva Consulting as a product for the Sattva Knowledge Institute (SKI). The authors take full responsibility for the contents and conclusions. Any participation of industry experts and affiliates who were consulted and acknowledged here, does not necessarily imply endorsement of the report's contents or conclusions. To quote this primer, please mention: Sattva Knowledge Institute, *Policy Landscape of India's Digital Public Infrastructure*, April 2023. Use of the report's figures, tables or diagrams, must fully credit the respective copyright owner where indicated. Reproduction must be in original form with no adaptions or derivatives. For use of any images in the report please contact the respective copyright holders directly for permission.

About Sattva Knowledge Institute

Sattva Knowledge Institute (SKI), established in 2022, is our official knowledge platform at Sattva. The SKI platform aims to guide investment decisions for impact, shedding light on urgent problems and high potential solutions, so that stakeholders can build greater awareness and a bias towards concerted action. Our focus is on offering solutions over symptoms, carefully curating strong evidence-based research, and engaging decision-makers actively with our insights. Overall, **SKI aims to shift intent and action toward greater impact by influencing leaders with knowledge.** All of our content proactively leverages the capabilities, experience and proprietary data from across Sattva.

Design: Usha Sondhi Kundu; cognitive.designs@gmail.com

CONTENTS

EXECUTIVE SUMMARY

The Government, on recognising the importance of digitisation as a means for effective delivery of public service, is facilitating the development of digital public goods through the creation of relevant policies and frameworks. This study aims to analyse the policies and frameworks that govern technological development in India to understand the principal areas of focus of the Government and potential implication for stakeholders.

Intervention areas

Government legislation is concentrated in four areas. A majority of the policies prioritised development of new technologies through innovation, along with risk management - both implying a focus on foundational development of the digital ecosystem in India, as well as establishment of standards for data protection and privacy within the emerging ecosystem. Several policies are also framed around data storing and sharing. These lay down standardised rules and mechanisms for consensual storage and sharing of data. There is minimal focus on content moderation policies at present – policies that govern and regulate content published on digital platforms to ensure a safe and secure digital space for users.

Sectors

The largest number of policies were observed to be sector-agnostic, including policies that enable setting standards for digital data sharing, interoperability and privacy, as well as policies that promote digitisation of service delivery processes across sectors (for example, policies enabling development of e-governance tools). A sizeable number of policies focus on the science and technology sector, particularly promoting innovation (for example, policies promoting technology and software products startups) and risk management (for example, policies protecting digital public infrastructure against cyber attacks). Special emphasis is laid on protection against potential leak of individuals' healthcare and financial data. Effort has been made to promote rights, equality and empowerment in the digital space (for example, policies facilitating universal, equal and unhindered access to electronics and ICTs products and services; and policies setting standards for permissible speech on the internet).

Enacting authorities

Multiple ministries at the Union level have enacted policies, guidelines, and frameworks to govern India's digital landscape, the most prominent among them being the Ministry of Electronics and Information Technology, followed by Ministries of Health and Family Welfare, Science and Technology, and Communications .

- The Ministry of Electronics and Information Technology is the main authority promoting e-development in India. It focuses on multiple intervention areas such as fostering innovation, risk management, data storing and sharing.
- The Ministries of Health and Family Welfare, Communications, and Science and Technology prioritise the protection of health-related data, and fostering innovation in the communications and science and technology sectors, respectively.

Opportunities for stakeholders

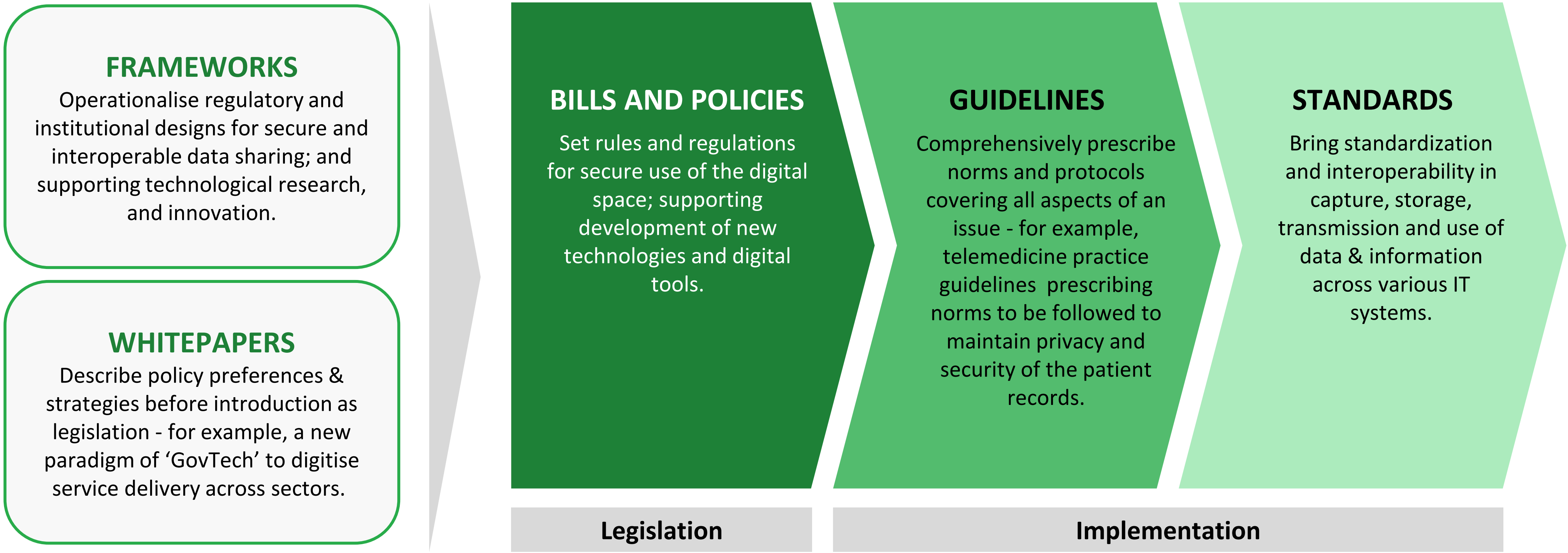
Philanthropic organisations, multilaterals, private sector players and non-profits have a proactive role to play in bringing about a digital transformation within the given legislative and regulatory ecosystem.

- Philanthropic organisations and multilaterals have the opportunity to provide relevant inputs to the government on policy development, design large scale technology adoption programmes, along with providing financial and capacity building support to technology developers. Multilaterals can additionally facilitate the development of global internet-related technical standards.
- Non-profits can develop awareness programmes to highlight the value of technology-based interventions and alleviate the fear of loss of data. They can also develop digital literacy programmes to enable users and service delivery agents to engage with the digital ecosystem.
- The private sector can leverage open-source technologies and open APIs, made easily accessible through the legislative framework, to innovate tech-based solutions and applications.

DIGITAL POLICIES LANDSCAPE

Frameworks and whitepapers help develop strategies on relevant challenges, and may give rise to bills and policies, which further leads to development of guidelines and standards to ensure effective implementation.

Types of government interventions in the digital ecosystem observed under this study



FRAMEWORKS

Operationalise regulatory and institutional designs for secure and interoperable data sharing; and supporting technological research, and innovation.

WHITEPAPERS

Describe policy preferences & strategies before introduction as legislation - for example, a new paradigm of 'GovTech' to digitise service delivery across sectors.

BILLS AND POLICIES

Set rules and regulations for secure use of the digital space; supporting development of new technologies and digital tools.

GUIDELINES

Comprehensively prescribe norms and protocols covering all aspects of an issue - for example, telemedicine practice guidelines prescribing norms to be followed to maintain privacy and security of the patient records.

STANDARDS

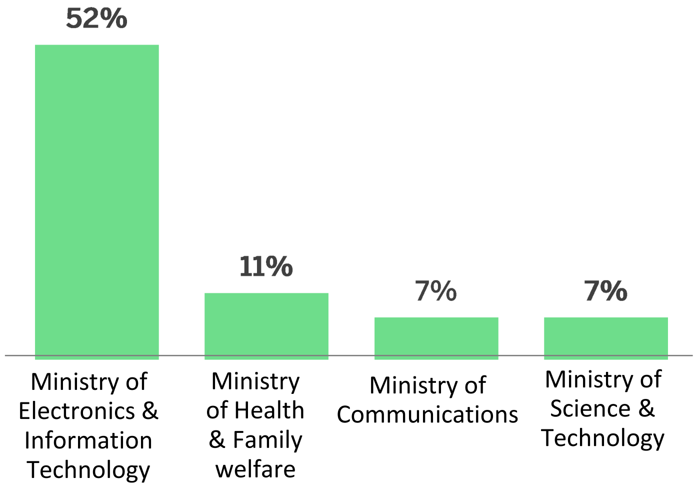
Bring standardization and interoperability in capture, storage, transmission and use of data & information across various IT systems.

Legislation

Implementation

The Indian government is prioritising the development of new technologies, along with their risk management; many policies are setting cross-sectoral standards for the digital ecosystem.

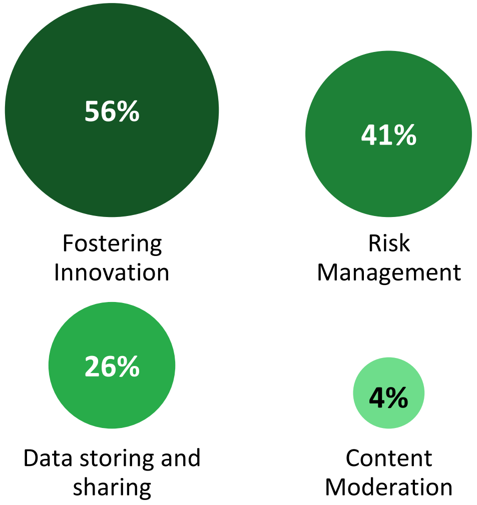
Policies, guidelines, frameworks, etc. enacted by government authorities…



Key insights

- The Ministry of Electronics and Information Technology, being the main authority promoting e-Development in India, focuses on fostering innovation, risk management, data storing and sharing.
- The Ministries of Communications, and Science and Technology focus on fostering innovation in digital ecosystem through legislation, while the Ministry of Health and Family Welfare prioritises protection of health data.
- Other authorities active are NITI Aayog, RBI, Ministries of Commerce & Industry, Education, Skill Development & Entrepreneurship, & National Medical Commission.

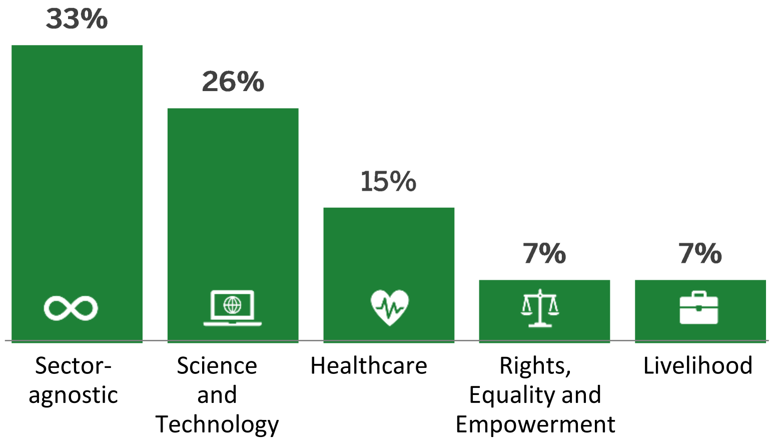
…aim to introduce the following interventions in the digital ecosystem…



Key insights

- Development of new technologies through policies encouraging innovation has been prioritised.
- There is equal focus on risk management within the emerging digital ecosystem — promoting policies that establish rules and regulations for protecting digital data, ensuring privacy and defending against cyber attacks.

…with applications across a range of sectors



Key insights

- Applications include setting foundational standards for digital data sharing, interoperability and privacy, along with the digitisation of service delivery processes in major sectors.
- Innovation is being fostered across domains such as science and technology (for example, policies promoting technology and software products startups), and sector-agnostic areas (such as policies enabling development of e-governance tools).
- There is special emphasis on protection against potential leak of individuals' financial data and medical records.
- Other sectors include education, finance and manufacturing.

Policies fostering innovation facilitate the creation and use of digital resources; risk management policies protect against cyber attacks, while others ensure secure data sharing and moderate online content.

FOSTERING INNOVATION

Policies support the creation and development of new technologies and digital tools by

- Facilitating the development and sharing of digital resources such as APIs and open source software that can be leveraged by actors in the country (including government and private players) to build digital platforms, tools and technologies
- Supporting capacity building for creation of new digital platforms, tools and technologies

Example: The policy on Adoption of Open Source Software for Government of India encourages use of open source software for creation of e-governance applications, by making source code freely available to study, modify and redistribute.

RISK MANAGEMENT

Policies set rules and regulations to ensure the protection of data and digital information architecture to prevent data leaks and misuse; they are also aimed at protecting the public and private infrastructure from cyber attacks.

Example: The National Cyber Security Policy aims to protect information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, and reduce vulnerabilities and minimise damage from cyber incidents.

DATA STORING AND SHARING

Policies lay down standardised **rules and mechanisms for recording or storing data and facilitating consensual sharing of individuals and organisations data** with relevant authorities.

Example: The National Data Sharing and Accessibility Policy aims to facilitate access to government-owned shareable non-sensitive data in a proactive and periodically updatable manner for wider accessibility and use of public data and information.

CONTENT MODERATION

Policies set **standards and rules for governing and regulating content published on digital platforms, to ensure a safe and secure digital space** for users.

Example: IT Rules (2022) aim to ensure greater diligence with respect to content on social media platforms, by appointing governmental committees to ensure non-circulation of copyrighted material and content that is defamatory, racially or ethnically objectionable, paedophilic, or threatening to India's sovereignty.

India's digital policy landscape includes policies, frameworks, guidelines, standards and white papers released by government authorities; six policies and one framework have been detailed under this study.

Policies (21)

- Digital Personal Data Protection Bill (2022)
- Digital Provisions in National Education Policy (2020)
- Digital Information Security in Healthcare Act (2018)
- Policy on Open Application Programming Interfaces (APIs) for Government of India (2015)
- Policy on Adoption of Open Source Software for Government of India (2014)
- National Data Sharing and Accessibility Policy (2012)

- Health Data Management Policy (Draft) (2022)
- Payment and Settlement Systems Regulations (2022)
- IT Amendment Rules (2022)
- Indian Telecommunication Bill (2022)
- National Data Governance Framework Policy (Draft) (2022)
- Science, Technology, and Innovation Policy (2020)
- National Policy on Electronics (2019)
- National E-Commerce Policy (Draft) (2019)
- National Policy on Software Products (2019)
- National Digital Communications Policy (2018)
- ICT enablement provisions in National Policy for Skill Development and Entrepreneurship (2015)
- Policy on Use of IT Resources of Government of India (2014)
- National Cyber Security Policy (2013)
- National Policy on Universal Electronic Accessibility (2013)
- National Policy on Information Technology (2012)

Frameworks (3)

- Data Empowerment And Protection Architecture Framework (2020)

- India Enterprise Architecture (IndEA) Framework (2017)
- ICT&E R&D and Innovation Framework (2013)

Guidelines (1)

- Telemedicine Practice Guidelines (2020)

Standards (1)

- Electronic Health Record Standards in India (2016)

White papers (1)

- Strategy for National Open Digital Ecosystems (2020)

▨ Detailed in this primer

POLICIES

National Data Sharing and Accessibility Policy

Policy Objective

The National Data Sharing and Accessibility Policy (2012) was formulated to enable the proactive and regular sharing of non-sensitive data collected or owned by the Government of India to aid decision making for national development.

Scope

The Policy applies to all data and information created, generated, collected and archived by entities using public funds either directly provided by GoI, or through authorised agencies.

Context

Accessible, credible and relevant data is crucial for decision making. Government data, if made available systematically, can increase transparency and unlock value by reducing duplication.

Policy Provisions

Department-wise classification of shareable and non-shareable data

Departments will produce list of non-shareable data (negative list) to be reviewed periodically. Shareable data will be further classified into open, registered and restricted access.

Setting up of an integrated data warehouse

Development of an integrated repository of metadata from various central ministries as part of data.gov.in which will eventually include data from states and union territories.

Standardisation of cross-departmental data sets

The Department of Information Technology will develop standards for data sets and metadata.

Implications for Digital Infrastructure

- Availability of all centrally generated data in one integrated portal (data.gov.in).
- Use of a standardised and machine-readable format for data sharing across ministries.
- Increased transparency by improved traceability of data through complete referencing.
- Data shared in this manner can serve as input for other digital platforms or data dashboards.

However, significant challenges exist regarding both the demand and supply of such open data (Agarwal 2016). Data sets are often either unavailable or are incomplete, duplicate, incorrectly referenced or provided in non-machine-readable formats that do not lend themselves to further analysis. They often cannot be used in conjunction with each other. Additionally, a study found that only 57% of research personnel surveyed were aware about open government data initiatives in India (Agarwal 2016).

Policy for Adoption of Open Source Software for Government of India

Policy Objective

The Policy for Adoption of Open Source Software (2015) was formulated to encourage the "formal adoption and use of open source software (OSS) in government organisations", in order to increase efficiency and control in digital infrastructure development.

Scope

Mandatorily applies to all government organisations at the Centre. State governments may adopt it voluntarily for all new e-governance applications and new versions of existing applications.

Context

The Digital India campaign requires large investments in the development of software infrastructure. Open source technologies are an effective way to reduce resource duplication and speed up the process.

Policy Provisions

Amendments to RFPs to include APIs	Central organisation RFPs for e-governance implementation will mandatorily include a clause to consider OSS as a preferred alternative to CSS. Suppliers will provide justification for OSS exclusion.
Conditions for the exclusion of OSS	Wherein OSS is not feasible due to specialised functional requirements, strategic importance or the lack of skilled personnel, exceptions may be considered.
Selection of proposals	Selection will be via OSS and CSS comparison on metrics such as capability, scalability, strategic control, security, life-time costs and support requirements.
Institutional support and ecosystem facilitation	GoI will strengthen OSS solutions by facilitating collaboration between academia, industry and the developer community, both locally and globally.

Implications for Digital Infrastructure

- Source code to be available free of royalty for all end-users to study, modify and redistribute.
- Increased competition in public procurement and reduced instances of vendor lock-in.
- Reduced total cost of ownership of digital infrastructure.
- Increased transparency and rigour of digital infrastructure through collaborative troubleshooting.
- Reduced probability of compromise and data breaches through quick bug detection and resolution.

* OSS: Open Source Software; CSS: Closed Source Software

Policy for Open Application Programming Interfaces (APIs) for Government of India

Policy Objective

The Policy for Open Application Programming Interfaces (APIs) encourages the formal adoption of APIs in government organisations to promote software interoperability.

Scope

Mandatorily applies to all government organisations at the Centre. State governments may adopt it voluntarily for all new e-governance applications and new versions of existing applications.

Context

Under Digital India, the government aims to create a seamless service delivery experience across multiple channels such as mobile, web, etc. This requires interoperability of data and processes.

Policy Provisions

Sharing of data using APIs	All relevant government data must be made available via open APIs in a machine-readable manner as per classification in the NDSAP (2012).
Standards for APIs	Every API is to be platform- and language-independent, free wherever possible, compatible with at least two previous versions of software and accompanied by sample code information for developers.
Security while using APIs	All APIs will comply with the National Cybersecurity Policy; any government application consuming data from others via APIs will follow information handling, authentication and authorisation mechanisms of publishing organisations.
Amendments to RFPs to include APIs	RFPs for e-governance application will contain a specific requirement to publish APIs to other government entities and the public domain.

Implications for Digital Infrastructure

- Increased interoperability between government data platforms, enabling the use of single sign on (SSO) , leading to increased user convenience.
- Efficient development of digital platforms and applications through a “building block" approach, leveraging already existing APIs.
- Increased number of players in digital infrastructure development, due to ability to build on existing APIs, leading to increased innovation and end-user satisfaction.

Data Empowerment and Protection Architecture (Draft for Discussion)

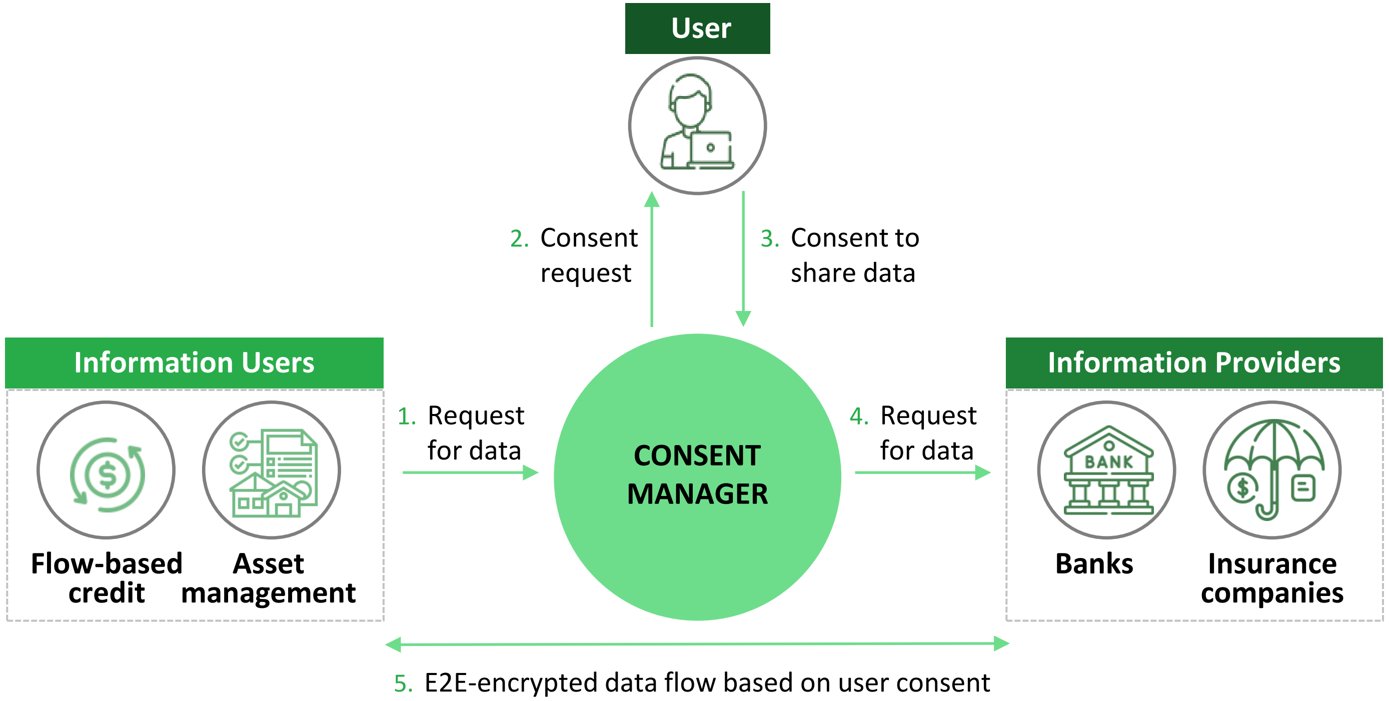
Policy Objective

Providing individuals with "practical means to access, control and selectively share personal data" stored across multiple datasets, thus maximising individual empowerment while reducing concerns of privacy and data misuse.

Context

Lack of harmonisation of data sharing standards within and across sectors and monopolisation of service delivery due to unequal access to user data.

A new entity called consent managers set up to manage the consent of data principals across multiple data fiduciaries in an accessible and transparent manner.



Note: In the case of the financial sector as depicted above, the consent managers are called Account Aggregators (AAs).

1. Based on a **consent artefact** that replaces blanket terms and conditions. The artefact is modelled on the **ORGANS** principles: **Open Standards, Revocable, Granular, Auditable, Notice to all parties, and Secure by Design.**
2. New consent managers can just "plug in" to existing systems via open APIs, instead of forming relationships with information providers.
3. Financial information standards empower data recipients to quickly interpret requests from new institutions.
4. Data fiduciaries cannot make provision of services conditional on consent.

DEPA forms the final layer of the India Stack, a set of digital public goods created to facilitate private sector participation in service delivery.

Data Empowerment Layer	DEPA
Payments Layer	UPI UNIFIED PAYMENTS INTERFACE
Identity Layer	AADHAAR

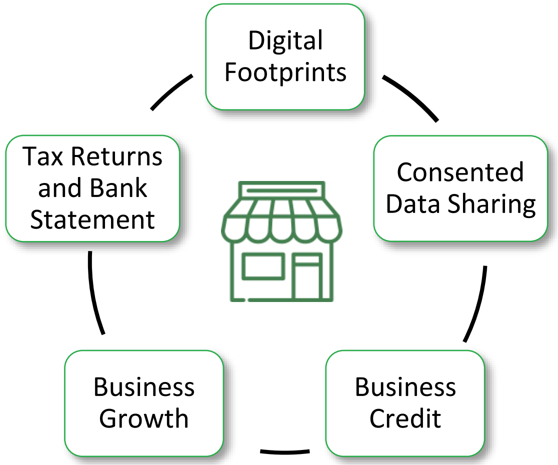
Data Empowerment and Protection Architecture (continued)

Advantages of DEPA

Increases individual empowerment: Better access to personal data and ability to manage consent at a granular level.

Spurs innovation among service providers: Barriers to entry are reduced as providers can plug into existing data-sharing rails using open APIs. They are hence forced to compete on the basis of products and UI/UX, rather than data access.

Drives financial inclusion: DEPA facilitates flow-based credit in lieu of traditional collateral-based credit models, empowering entities to share their financial history with lenders and helping to plug the INR 20-25 trillion credit gap faced by MSMEs (RBI 2019).



Use Cases/Implications of DEPA for Digital Infrastructure

वित्त मंत्रालय MINISTRY OF FINANCE	DEPA went live in the financial sector under RBI, MoF, SEBI, PFRDA and IRDAI. So far, seven account aggregators (AAs) have been licensed. A non-profit collective, called Sahamati has been set up to strengthen the AA ecosystem.
GSTN	GSTN is the first major government department to be onboarded onto the AA ecosystem as an information provider, in order to enable cash flow-based lending.
national health authority	The NHA first used DEPA in 2020 as part of National Digital Health Mission.
कौशल विकास और उद्यमशीलता मंत्रालय MINISTRY OF SKILL DEVELOPMENT AND ENTREPRENEURSHIP	The MSDE advocated for the use of DEPA in the creation of a digital skill credential, to share verified information about training and work experience.
TRAI	Telecom companies are also set to become information providers and users in the AA ecosystem, following a partnership announcement with TRAI in August 2020.
Ministry of Housing and Urban Affairs Government of India	The proposed Urban Data Exchange would also potentially leverage DEPA for data sharing.

Digital Personal Data Protection Bill

Policy Objective

Providing for the processing of digital personal data while recognising the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes. It lays down the rights and duties of citizens and duties/obligations of Data Fiduciary on the use of data.

Scope

Applies to the processing of digital personal data within the territory of India (when it is collected from Data Principals online; or collected offline, but is digitised); and outside the territory of India (if in connection with an activity of offering goods or services to Data Principals within the territory of India).

Context

Unchecked processing of personal data may have adverse implications for the privacy of individuals. Currently, India does not have a standalone law on data protection, and the usage of personal data is regulated under the Information Technology (IT) Act, 2000, which is considered inadequate to ensure the protection of personal data.

Policy Provisions

Establishes consent sharing mechanism for data processing

Personal data is processed only for a lawful purpose for which consent is given, and it may be withdrawn at any point in time. Consent will be deemed given in certain cases. For those below 18 years of age, consent will provided by a guardian.

Prescribes role and duties of data fiduciary

The data fiduciary will ensure accuracy of data, build security safeguards and cease to retain personal data when the purpose has been met (storage limitation). Storage limitation requirement will not apply for processing by government.

Lays down rights and duties of data principals (citizens)

Data principals have the right to obtain information about processing, seek correction/erasure of personal data, grievance redressal, and so on. At the same time, they must not register a false complaint or suppress information.

Notifies provisions for data transfer outside India

The central government will notify countries where data may be transferred. Rights of data principals and obligations of data fiduciaries (except data security) will not apply in specified cases (for example, prevention of offenses).

Establishes compliance framework (Data Protection Board of India)

The Data Protection Board of India will monitor compliance, impose penalties, direct data fiduciaries to take necessary measures in the event of data breach, and hear grievances made by affected persons.

Implications for Digital Infrastructure

- Expands scope of the data principal's right to privacy by extending to them the right to withdraw consent at any point.
- Personal data of children that may cause harm to a child will not be processed. The data fiduciary shall not undertake tracking or behavioral monitoring of children or targeted advertising directed at children.
- Companies will be required to stop retaining user data if it no longer serves the business purpose for which it was collected. Users shall have the right to correction and erasure of their personal data.
- Relaxes rules on cross-border data flows, permits data transfer to select global destinations which is likely to foster bilateral trade agreements and easier compliance requirements for start-ups.

Digital Provisions in the National Education Policy

Objective

The National Education Policy (2020) recognises the important bidirectional relationship between technology and education. The implementation of Digital India will need a technologically literate workforce; however, technology itself can be facilitator of accessible and quality education.

Establishment of NETF

- An autonomous body, the National Educational Technology Forum (NETF) is to be created to build ed-tech capacity.
- NETF will categorise emergent technologies based on disruptive potential and advise central and state agencies.

Facilitating digital literacy

- Higher education institutions (HEIs) will create preliminary versions of online courses and evaluate impact.
- Universities shall aim to offer postgraduate and PhD programmes in Artificial Intelligence/Machine Learning (AI/ML) and their applications in agriculture, healthcare, etc.
- School education will also cover AI and its ethical ramifications.

Strengthening existing platforms and creation of new ones

- Policy voices need to create open and interoperable ed-tech for better learning and assessment.
- Central Institute of Information Technology will promote Digital Infrastructure for Knowledge Sharing (DIKSHA) and other initiatives.
- DIKSHA will house content in all regional languages created by various boards and be better integrated with the curriculum. Better methods to monitor student progress are advised.
- DIKSHA, SWAYAM, and others. to include user ratings. Inclusion of virtual labs is advised.

Ensuring accessibility and quality of digital education

- A unit for building digital infrastructure, content and capacity to be set up within the MHRD.
- NETF and others are advised to conduct pilot evaluations on integration of offline and online education and address digital divide and other risks. They are also advised to set standards for online content, technology and pedagogy.
- Teacher training on digital content creation is recommended.

Implications for Digital Infrastructure

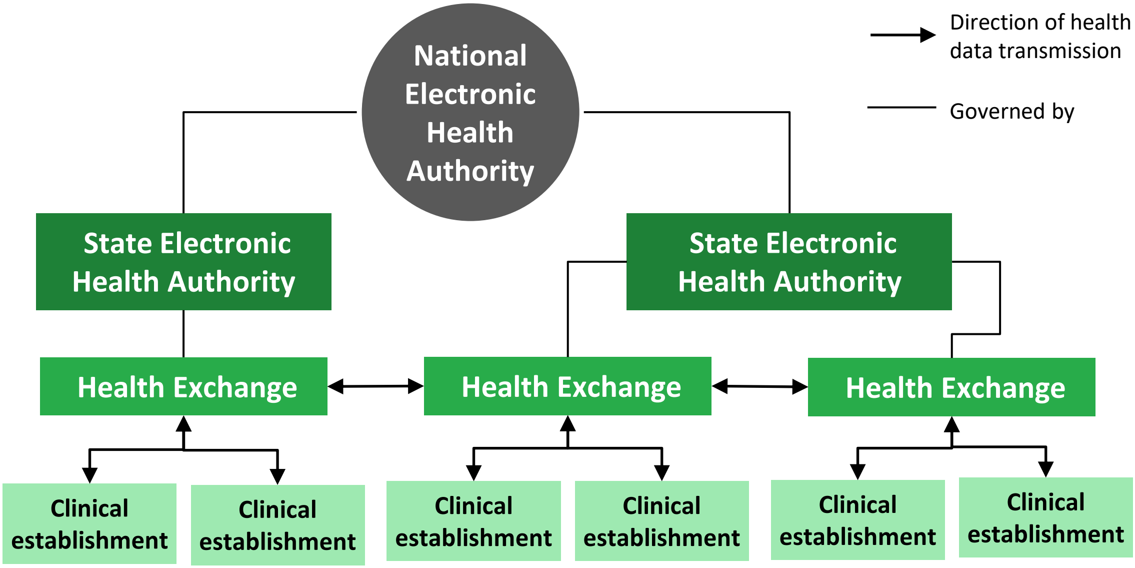
- Digital platforms in education will utilise new technologies such as AI and become more user-centric and accessible, increasing their efficacy both for learning and assessment.
- A technologically literate workforce will be created to spur the development of future digital platforms.

Digital Information Security in Healthcare Act (Public Consultation Draft)

Policy Objective

The Digital Information Security in Healthcare Act (2017) seeks to standardise and regulate the “collection, storing, transmission and use of digital health data; and to ensure reliability, data privacy, confidentiality and security” of such data. The provisions of the Act will be applicable pan-India, except in Jammu and Kashmir.

Establishment of Electronic Health Authorities, Executive Committees and Health Exchanges



National Electronic Health Authority

State Electronic Health Authority

State Electronic Health Authority

Health Exchange

Health Exchange

Health Exchange

Clinical establishment

Clinical establishment

Clinical establishment

Clinical establishment

Clinical establishment

Clinical establishment

→ Direction of health data transmission

— Governed by

Executive Committees will be set up to assist Electronic Health Authorities at both the nation and state-levels.

A clinical establishment, health information exchange, National or State Electronic Health Authority or any other establishment that generates and collects digital data “shall be duty bound to protect the privacy, confidentiality, and security” of the same.

Rights and Responsibilities of the National Electronic Health Authority

- Develop standards, protocols and operation guidelines for generation, collection, storage and transmission applicable to any organisations with data access.
- Ensure data protection and prevent theft or breach.
- Establish security measures such as access controls, encrypting and audit trials to ensure data protection at every stage (generation, collection, storage and transmission).
- Conduct periodic audits of health exchanges to ensure compliance to the Act. The Authority can access physical or virtual infrastructure and records of health information exchanges at any time.
- Develop protocol for the international transmission of data.

Rights and Responsibilities of State Electronic Health Authorities

- Ensuring that clinical establishments and other organisations collect, store, transmit and use data in accordance with the Act.
- Accessing premises and records of clinical establishments at any time to ensure compliance.

Rights and Responsibilities of Health Exchanges and Clinical Establishments

- Exchanges will maintain a register to record any data transmission.
- Clinical establishments and exchanges to also record the purposes and use of all data accessed.
- Clinical establishments may retain a copy for reasonable use before transmitting encrypted data to exchanges.

Digital Information Security in Healthcare Act (continued)

Rights of Data Owners

1. Right to consent to the generation, collection, storage and transmission of digital data and not be refused services on grounds of non-consent.
2. Right to privacy, confidentiality, and security of digital data and to prevent any disclosure that might cause damage to themselves.
3. Right to ensure that data collected is specific, relevant and not excessive.
4. Right to rectify incorrect data within 3 days of written application.
5. Right to be aware of the clinical establishments or entities and recipients who have/may have access.
6. Right to be notified of every instance when their data is accessed.
7. Right to access their own digital data with details of consent given and data accessed by any entity.
8. Right to give or withdraw consent for each instance of transmission or use of data in an identifiable form.
9. Right to ensure that nominated individuals/family have emergency data access.

Purpose of collection, storage, transmission and use of health data

1. To advance delivery of care. Personally identifiable data can only be used for this purpose.
2. To enable early identification and rapid response to outbreaks.
3. To aid early detection, prevention and management of chronic diseases.
4. To undertake academic research.

Standards for data use and privacy

- ✗ No clinical establishment can collect data for digital conversion, unless in accordance with the Act.
- ✗ No data, either identifiable or anonymised, must be shared with employers, HR consultants, pharmaceutical companies or others for any commercial purpose. Insurance companies can avail data for processing claims after seeking owner consent, but must not insist on access.
- ✓ All health exchanges and clinical establishments will train staff regularly to ensure compliance with security standards.
- ✓ Owners must be notified within three working days, in case of a data breach.
- ✓ Courts can access data for administration of justice, and government departments can avail anonymised data upon request.

Implications for Digital Infrastructure

Any digital platform set up by a clinical establishment/healthtech products that access health data from clinical establishments must comply with the Act.

OPPORTUNITIES FOR STAKEHOLDERS

NGOs can undertake awareness generation interventions to alleviate data privacy concerns, and to ensure digital readiness; multilaterals and philanthropies could provide financial and technical support for innovation.

Opportunities for the ecosystem

NGOs

Develop awareness generation programmes	Develop awareness programmes by presenting potential use cases that illustrate the value of technology-based interventions, and alleviate fears around the loss of data and privacy.
Develop digital literacy programmes	Develop digital literacy programmes to enable individuals to engage with the digital ecosystem, both as users and agents of service delivery.
Ensure digital readiness	Play a catalytic role to ensure that the end-beneficiaries are prepared to adopt new technologies and DPGs, by increasing access to necessary resources.
Provide technical insight for developers	Develop a larger range of use cases outlining digital tools and applications to be developed, to provide insight to technology developers and enable them to better conceptualise solutions.
Adopt DPGs in own operations	NGOs will act as active users/adopters of DPGs in their operations, in addition to their efforts to promote adoption of DPGs among end beneficiaries.

Multilaterals and Philanthropic Foundations

Develop technology adoption programmes	Design and manage programmes that involve large-scale adoption of technology-based products.
Foster tech-based innovation	Provide financial, technical and capacity-building support to technology developers for the development of inclusive, and low-cost new products and services.
Facilitate standards development	Facilitate development of global internet-related technical standards, best practices and international cooperation on digital policies.

Private Sector

Foster tech-based innovation	Leverage the increased opportunity to develop technology solutions and applications leveraging open-source technology and APIs.
Engage in dialogue through consortiums	Leverage business consortiums to discuss the potential applications of DPGs in businesses and development of industry standards relating to digitisation.

REFERENCES

- Agarwal, N 2016, *Unleashing the full potential of India's 'Open Government Data' initiative*, Ideas for India.
- Bohannon, M 2015, *India adopts a comprehensive open source policy*, Open Source.com.
- Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry, Government of India (2019), *National e-Commerce Policy (Draft)*.
- Department of Science and Technology, Government of India 2012, *National Data Sharing and Accessibility Policy*.
- Department of Telecommunications, Government of India 2018, *National Digital Communications Policy*.
- Department of Telecommunications, Government of India (2022), *Indian Telecommunication Bill*.
- Goled, S 2021, *The State Of Open-Source Ecosystem In India*, Analytics India.
- Ministry of Health and Family Welfare, Government of India [MoHFW] 2017, *Digital Information Security in Healthcare Act* (Draft for Public Consultation).
- MoHFW (2016), *Electronic Health Record Standards in India*.
- MoHFW 2022, *Draft Health Data Management Policy*.
- Ministry of Education, Government of India (2020), *National Education Policy*, pp. 56-60.
- Ministry of Electronics and Information Technology, Government of India [MeitY] 2012, *National Policy on Information Technology*.
- MeitY 2013a, *National Policy on Universal Electronic Accessibility*.
- MeitY 2013b, *ICT&E R&D and Innovation Framework.*
- MeitY 2013c, *National Cyber Security Policy*.
- MeitY 2014a, *Policy on Adoption of Open- Source Software for Government of India*.
- MeitY 2014b, *Policy on Open Application Programming Interfaces (APIs) for Government of India*.
- MeitY 2014c, *Policy on Use of IT Resources of Government of India*.
- MeitY 2017, *India Enterprise Architecture (IndEA) Framework*.
- MeitY 2019a, *National Policy on Electronics*.
- MeitY 2019b, *National Policy on Software Products*.
- MeitY 2020, *Strategy for National Open Digital Ecosystems (Consultation Whitepaper)*.
- MeitY 2022a, *The Digital Personal Data Protection Bill (Draft)*.
- MeitY 2022b, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*.
- MeitY 2022c, *National Data Governance Framework Policy (Draft)*.
- Ministry of Skill Development and Entrepreneurship, Government of India (2015), *National Policy for Skill Development and Entrepreneurship*.
- Ministry of Science and Technology, Government of India (2020), *Science, Technology, and Innovation Policy*.
- National Medical Commission 2020, *Telemedicine Practice Guidelines*
- NITI Aayog, Government of India 2020, *Data Empowerment and Protection Architecture* (Draft for Discussion).
- Reserve Bank of India (2019), *The Payment and Settlement Systems Amendment Act*.
- Sahamati n.d.a, *Home Page*, viewed on 13 October, 2022.
- Sahamati n.d.b, *Mission*, viewed on 13 October, 2022.