



A Paradigmatic Shift in Public Service Delivery: Inclusive, Efficient and Secure DPI

SEPTEMBER
2026

A Paradigmatic Shift in Public Service Delivery: Inclusive, Efficient and Secure DPI

This report is an output of the project titled “A Paradigmatic Shift in Public Service Delivery: Accessible, Inclusive and Secure DPI,” undertaken by ICRIER in collaboration with UQ Cyber Research Centre, University of Queensland, and supported by a grant under the Australia-India Cyber and Critical Technology Partnership (AICCTP) of the Department of Foreign Affairs and Trade, Government of Australia.

Copyright © 2026 by Indian Council for Research on International Economic Relations (ICRIER) and University of Queensland (UQ)

Prepared by: ICRIER and UQ Cyber Research Centre, University of Queensland

ICRIER Team: Payal Malik, Nikita Jain, Bhargavee Das, Shiva Kanwar, Mehak Aggarwal, Krishnapriya VS

UQ Team: Priyanka Singh, Luhut Sinambela

All Rights Reserved

No part of this report shall be reproduced, stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the copyright holder(s) and/or publishers.

Disclaimer: *Opinions and recommendations in the report are exclusively of the author(s) and not of any other individual or institution, including ICRIER. This report has been prepared in good faith on the basis of information available at the date of publication. All interaction and transactions with industry sponsors and their representatives have been transparent and conducted in an open, honest and independent manner as enshrined in ICRIER Memorandum of Association. ICRIER does not accept any corporate funding that comes with a mandated research area which is not in line with ICRIER’s research agenda. The corporate funding of an ICRIER activity does not, in any way, imply ICRIER’s endorsement of the views of the sponsoring organisation or its products or policies. ICRIER does not conduct research that is focused on any specific product or service provided by the corporate sponsor.*

Acknowledgements

This report is an output of the project “A Paradigmatic Shift in Public Service Delivery: Accessible, Inclusive and Secure DPI,” supported by a grant under the Australia-India Cyber and Critical Technology Partnership (AICCTP) of the Department of Foreign Affairs and Trade (DFAT), Government of Australia. The report has been prepared by ICRIER in partnership with the UQ Cyber Research Centre, University of Queensland. We are grateful to DFAT for their support across the full programme of work.

The analysis draws substantially from three stakeholder engagements convened under the project. The first, a “Transformation of Health Systems through Digital Public Infrastructure” workshop, was convened by ICRIER in partnership with the University of Queensland and the ICRIER Prosus Centre for Internet and Digital Economy (IPCIDE) in New Delhi and brought together experts for a full-day dialogue on the Ayushman Bharat Digital Mission. We thank the keynote speakers, Ram Sewak Sharma (Former CEO, National Health Authority), Clair Sullivan (Director, Queensland Digital Health Centre, University of Queensland), Satyanarayana Jeedigunta (DPI Academy, Artha Global, C4IR India, and World Economic Forum) and Vinayak Godse (CEO, Data Security Council of India) as well as Vikram Pagaria (Director, National Health Authority) for his special address. We are also grateful to the participants: Neelesh Kapoor, Oshia Garg, Siddhartha Bhattacharya, Aditya Patkar, Sri Vidhya Bhavani Munuswamy, Harsh Parikh, Abhishek Gautam, Pallavi Gupta, Surajit Nundy, Vikas Kharbanda, Akshat Mandloi, Prem Kumar, Kavitha Palaniappan, Padmini Vishwanath, Sunita Nadhamuni, Pankaj Gupta, Apoorva Gupta, Daniel Buckley, Bodhish Thomas and Shiffali Singla. Additionally, we would like to thank the Office of the State Mission Director, Andhra Pradesh, specifically G Veerapandian, Susmita Dexeena, Hasini, S Sreedhar, Srikanth, Yuvarajan Subramaniam, Charan Tej and Mallikarjuna. Between them, they represented the National Health Authority and state Ayushman Bharat Digital Mission (ABDM) missions, health technology firms, industry bodies, multilateral organisations, academic institutions and civil society.

The second, a workshop on “Digital Public Infrastructure and Public Service Delivery: Inclusion. Efficiency. Security.,” also held at New Delhi, examined the Direct Benefit Transfer (DBT) ecosystem. We thank Saurabh K Tiwari (Additional Secretary, DBT Mission) for the keynote address, V Anantha Nageswaran (Chief Economic Adviser, Government of India) for the distinguished address and Rajesh Bansal (Former CEO, Reserve Bank Innovation Hub) and Rajeev Shorey (Director, IIIT Surat) for their special addresses. We are grateful to the expert panellists: Abhishek Singh, Anita Gurusurthy, Ankit Mishra, Arijit Chakraborti, Arjita Madan, Ayushi Khare, Beni Chugh, Kunal Raj Barua, Nikita Kwatra, Nish Perera, Pranay Sinha, Radhika Agashe, Rajendran Narayanan, Rakesh Maheshwari, Sandeep Kumar Shukla, Shivangi Rai, Shweta Banerjee, Sridhar Dhulipala, Srinivas Kodali, Sunaina Kumar and Sunil Kulkarni, drawn from the DBT Mission, Unique Identification Authority of India (UIDAI), research institutions,

philanthropic organisations, industry associations and civil society. We are also grateful to the Gates Foundation for its support for this workshop.

We owe a particular debt to those who helped shape these two workshops and secure the participation that made them substantive: Anshuman Kamila and Sumita Kale for the workshop on Direct Benefit Transfer, and Himanshu Burad and Sundeep Agarwal for the workshop on digital health.

The third engagement, an expert feedback conference on “Governing for Trust: Inclusive, Efficient, and Secure Digital Public Infrastructure,” was hosted by the UQ Cyber Research Centre in partnership with ICRIER at the University of Queensland, Brisbane City. The programme comprised keynote addresses, a presentation of the draft report and its evaluative framework, a structured panel across the report’s three pillars and lightning talks. We thank the keynote speakers, Ryan Ko, Xue Li, Fiona Hinchliffe, Ivano Bongiovanni and Natalie Smith; Stan Karanasios, David Stockdale and Tim Reddel, who joined Ivano Bongiovanni and Natalie Smith on the feedback panel; and the lightning talk presenters, Angga Septananda and David Gaul. We are grateful to all participants from government, healthcare, industry, civil society and the university, including colleagues from the UQ Cyber Research Centre, the UQ Business School, the UQ School of Electrical Engineering and Computer Science, the Institute for Social Science Research, the Queensland Digital Health Centre, AUSCERT and Mater. The feedback offered that day has been incorporated in this report.

We are equally grateful to the officials, practitioners, technologists, clinicians, industry representatives, civil society organisations and ecosystem participants in India and Australia who gave their time to interviews and consultations over the course of the research and who shared operational details that are not otherwise available in the public record.

We would also like to thank Smriti Parsheera and Harsh Shah for reviewing the chapter on the Ayushman Bharat Digital Mission and Sumita Kale for reviewing the chapter on Direct Benefit Transfer. Their comments improved both the analysis and its presentation.

We also thank Katie Williams and Gagandeep Singh for organising the feedback conference, Maria Khan and Shailly Gupta for their contributions to the workshops and their outputs, and Moksh Mehta for his contribution to chapter four. We also acknowledge Neha Arora, Raj Kumar Shahi and Rajesh Chaudhary for logistics and event management, Rajesh Chaudhary for design and Aswathy Gopinath for copyediting.

In keeping with the consultative character of these engagements, no view expressed in this report is attributed to any individual participant, and participation does not imply endorsement of the findings or recommendations. Responsibility for the analysis, and for any errors that remain, rests with the authors.

Table of Contents

Executive Summary	i
Abbreviations.....	iii
Glossary of Terms	vii
1. Introduction	1
1.1 <i>What is DPI?</i>	3
1.2 <i>DPI in Public Service Delivery</i>	5
2. Evaluative Framework for DPI in Public Service Delivery.....	7
2.1 <i>Pillar 1: Accessibility and Inclusivity.....</i>	9
2.2 <i>Pillar 2: Efficiency.....</i>	12
2.3 <i>Pillar 3: Security</i>	14
2.4 <i>Using the Framework for Holistic Assessment of DPI</i>	17
3. Case Study: Direct Benefit Transfer	18
3.1 <i>Introduction</i>	18
3.2 <i>Technical Architecture</i>	21
3.3 <i>Governance of the DBT Stack.....</i>	22
3.3.1 <i>Constitutional Governance of Digital Identity: Aadhaar’s Legal Evolution ..</i>	23
3.3.2 <i>Regulatory Governance of the DBT Ecosystem.....</i>	24
3.3.3 <i>Private-Sector Participation in the DBT Ecosystem</i>	25
3.4 <i>Accessibility and Inclusivity.....</i>	26
3.4.1 <i>Entry and Access Stage</i>	27
3.4.2 <i>Beneficiary Identification and Eligibility</i>	28
3.4.3 <i>Payment Processing and Authentication.....</i>	30
3.4.4 <i>Last-Mile Access: BCs, AePS and Cash-Out Infrastructure.....</i>	30
3.4.5 <i>Grievance Redressal.....</i>	32
3.4.6 <i>Inclusion–Exclusion Trade-Offs</i>	32
3.5 <i>Efficiency and Performance</i>	33
3.5.1 <i>Fiscal and Transaction Efficiency</i>	33
3.5.2 <i>Time and User-Side Efficiency.....</i>	36
3.5.3 <i>From Transfer Efficiency to Outcome Effectiveness</i>	36
3.6 <i>Security, Privacy and Cybersecurity</i>	37
3.6.1 <i>Privacy and Data Protection</i>	38
3.6.2 <i>Cybersecurity Risks and System Vulnerabilities</i>	39
3.6.3 <i>Fraud Risks</i>	40
3.6.4 <i>Cloud Infrastructure, Data Storage and Emerging Risks</i>	41

3.6.5	<i>Grievance Mechanisms for Security Breaches</i>	<i>42</i>
3.7	<i>Recommendations</i>	<i>43</i>
3.8	<i>Comparative Analysis: DPI-Enabled Welfare Delivery in India and Australia.....</i>	<i>46</i>
3.9	<i>Conclusion</i>	<i>50</i>
4.	Case Study: Ayushman Bharat Digital Mission	51
4.1	<i>Introduction</i>	<i>51</i>
4.2	<i>Technical Architecture</i>	<i>57</i>
4.2.1	<i>Inclusivity in Design.....</i>	<i>58</i>
4.2.2	<i>Limitations of the Architecture</i>	<i>60</i>
4.3	<i>Governance</i>	<i>61</i>
4.3.1	<i>Decentralised Governance and Multi-Stakeholder Coordination</i>	<i>62</i>
4.3.2	<i>Policy Foundations and Health Data Governance</i>	<i>64</i>
4.3.3	<i>Grievance Redressal.....</i>	<i>66</i>
4.4	<i>Efficiency.....</i>	<i>67</i>
4.5	<i>Privacy and Security.....</i>	<i>68</i>
4.5.1	<i>Privacy by Design</i>	<i>68</i>
4.5.2	<i>User Control and Rights</i>	<i>71</i>
4.5.3	<i>Cybersecurity.....</i>	<i>71</i>
4.6	<i>Recommendations</i>	<i>72</i>
4.7	<i>Comparative Analysis: DPI-Enabled Healthcare Provisioning in India and Australia.....</i>	<i>75</i>
4.8	<i>Conclusion</i>	<i>79</i>
5.	Key Lessons for DPI-Enabled Public Service Delivery	80
	Annexure 1: DPI for Public Service Delivery Assessment Framework	84
	Annexure 2: Direct Benefit Transfer Scheme in India	88
	Annexure 3: Ayushman Bharat Digital Mission (ABDM).....	91

List of Tables

Table 1: Select Definitions of DPI.....	4
Table 2: Overview of DPI for the Public Service Delivery Assessment Framework.....	8
Table 3: DBT Architecture Through the Lens of DPI Principles	20
Table 4: Strategic Priorities for the Next Phase of DBT	44
Table 5: Three-Pillar Comparison of India’s and Australia’s DPI Architectures for Welfare Delivery	47
Table 6: Traditional Digitalisation vs. DPI-H	52
Table 7: ABDM Components and Their Value Propositions	53
Table 8: Key Attributes of the Consent Artefact	69
Table 9: Comparing India’s and Australia’s DPI Architectures for Healthcare Provisioning ..	75

List of Figures

Figure 1: Structure of the Framework	7
Figure 2: Status of India’s DBT System as of 2026	19
Figure 3: DBT as a Layered DPI Stack	21
Figure 4: End-to-End Process Flow of DBT	22
Figure 5: Evolution of Aadhaar in India: Key Milestones.....	23
Figure 6: Efficiency Gains Through Aadhaar-Authenticated Direct Benefit Transfers	34
Figure 7: The ABDM Ecosystem	55
Figure 8: Cumulative Growth of ABHA Creation and Linkage of Health Records.....	56
Figure 9: ABDM Technical Architecture	57
Figure 10: Multi-Stakeholder Coordination in the 100 Microsite Project	63
Figure 11: Evolution of the Policy and Governance Framework of ABDM	65

List of Boxes

Box 1: The Debate on Private Access to Aadhaar	26
Box 2: Identity Does Not Imply Eligibility	29
Box 3: Post-Quantum Cryptography and Risks to the DBT system	42

Executive Summary

Digital Public Infrastructure (DPI) has emerged as the new paradigm in public service delivery, marking a shift from the digitisation of individual government services towards the creation of shared, interoperable digital foundations – identity, payments and data exchange – that can be reused across sectors by multiple stakeholders. Where earlier e-governance initiatives frequently produced fragmented, siloed systems that replicated existing bureaucratic structures rather than transforming them, DPI reimagines the role of the state from merely providing digital services to stewarding foundational infrastructure that enables innovation, coordination and integrated service delivery.

This report assesses how DPI performs in public service delivery, with a focus on the welfare distribution and healthcare sectors, which have significant differences in their service delivery. It examines India's Direct Benefit Transfer (DBT) and Ayushman Bharat Digital Mission (ABDM), alongside Australia's welfare delivery and My Health Record systems, using an original evaluative framework organised around three overarching pillars that together capture the fundamental objectives and trade-offs in DPI systems: Accessibility and Inclusivity; Efficiency; and Security.

The framework recognises that these dimensions are mutually reinforcing. Systems that prioritise only one dimension may inadvertently weaken the other dimensions; for example, stringent security requirements may create barriers to access, and efficiency gains achieved without adequate safeguards can undermine privacy, trust and long-term system resilience. Managing these trade-offs is a key challenge in the design and implementation of DPI-enabled public services.

The case studies illustrate two structurally different relationships between DPI and service delivery. DBT is best understood as a use case – a programme that leverages existing foundational DPI layers, principally Aadhaar-linked identity and payments, to disburse welfare entitlements directly to beneficiaries. ABDM, by contrast, represents a sectoral DPI, establishing a dedicated identity layer (the health ID), a registry of facilities and providers, and interoperability standards for electronic health records that other healthcare applications can build on. The two cases highlight the difference between DPI as foundational and DPI-enabled use cases built on top of infrastructure designed for other purposes.

India's experience demonstrates how foundational DPIs such as Aadhaar, UPI, and the Account Aggregator can be deployed at population scale to strengthen public service delivery in a large and diverse country. Australia illustrates how mature administrative institutions, strong regulatory frameworks and rights-based governance can support trusted digital public services within a federated governance system. Together, these cases provide a broad spectrum of experiences that generate lessons applicable to countries at different stages of digital transformation. Rather than identifying a single model for replication, the comparative

assessment demonstrates how different institutional pathways can achieve similar public service objectives even under differing administrative, legal and socioeconomic contexts.

The two case studies demonstrate that DPI's value for public service delivery depends not only on the sophistication of the underlying technology but also on its alignment with the service delivery ecosystem, its usability for stakeholders, the capacity and quality of relevant institutions and governance frameworks and the robustness of available privacy and security safeguards necessary for building public trust in the system. The comparative analysis across key design and implementation dimensions can enable countries to understand and evaluate the suitability of DPI in their local contexts.

DPI should be viewed as an evolving infrastructure shaped by regulatory reform, institutional learning, implementation feedback and technological adaptation. While interoperable digital infrastructure can substantially improve the scale, quality and responsiveness of government services, its long-term success depends on continuous institutional learning, adaptive governance and sustained public trust. As countries increasingly explore DPI across sectors, the central challenge is not simply to digitise public services but to build governance systems capable of delivering accessible, inclusive, efficient and secure outcomes within their own institutional and societal contexts.

Abbreviations

ABDM	Ayushman Bharat Digital Mission
ABHA	Ayushman Bharat Health Account
ADV	Aadhaar Data Vault
AePS	Aadhaar-enabled Payment Systems
AePDS	Aadhaar-enabled Public Distribution System
AIIMS	All India Institute of Medical Sciences
ANM	Auxiliary Nurse Midwife
APBS	Aadhaar Payment Bridge System
API	Application Programming Interface
ASHA	Accredited Social Health Activists
ATMs	Automated Teller Machine
AUA	Authentication User Agency
BCs	Business Correspondents
BPL	Below Poverty Line
CAG	Comptroller and Auditor General
CERT-IN	Indian Computer Emergency Response Team
CHO	Community Health Officer
CICO	Cash-in-cash-out services
CIDR	Central Identities Data Repository
CPGRAMS	Central Public Grievance Redressal and Monitoring Systems
CRQCs	Cryptographically Relevant Quantum Computers
CSCs	Common Service Centres
DBT	Direct Benefit Transfer
DBTL	Direct Benefit Transfer for LPG
DHIS	Digital Health Incentive Scheme
DHIS 2	District Health Information Software 2
DISHA	Digital Information Security in Healthcare Act
DPDP Act	Digital Personal Data Protection Act
DPI	Digital Public Infrastructure

EHR	Electronic Health Records
FHIR	Fast Healthcare Interoperability Resources
G2P	Government-to-Person
GCCs	Government Community Clouds
HDMP	Health Data Management Policy
HFR	Health Facility Registry
HIE-CM	Health Information Exchange-Consent Manager
HMIS	Hospital/Health Management Information System
HPR	Health Professional Registry
I4C	Indian Cyber Crime Coordination Centre
IEC	Information, Education and Communication
IPPB	Indian Post Payments Banks
ISO	International Organization for Standardization
JAM	Jan Dhan–Aadhaar–Mobile
KUA	e-KYC User Agencies
KYC	Know Your Customer
LMIC	Low- and Middle-Income Country
LMIS	Laboratory Management Information System
LPG	Liquefied Petroleum Gas
MeitY	Ministry of Electronics and Information Technology
MIS	Management Information Systems
MoU	Memorandum of Understanding
NACH	National Automated Clearing House
NCIIPC	National Critical Information Infrastructure Protection Centre
NHA	National Health Authority
NHCX	National Health Claims Exchange
NPCI	National Payment Corporation of India
ONORC	One Nation, One Ration Card
OPD	Out Patient Department
OTP	One Time Password

PDS	Public Distribution System
PFMS	Public Financial Management System
PHR	Personal Health Record
PM-JAY	Pradhan Mantri Jan Arogya Yojana
PMJDY	Pradhan Mantri Jan Dhan Yojana
PoS	Point of Sale
PQC	Post Quantum Cryptography
RBI	Reserve Bank of India
RCH	Reproductive and Child Health
SECC	Socio-Economic and Caste Census
SIR	Special Intensive Revision
SITAA	Security and Trust in AI
SWIK	Social Welfare, Innovation, Knowledge
UHI	Unified Health Interface
UID	Unique Identification / Unique Identifier
UIDAI	Unique Identification Authority of India
UPI	Unified Payments Interface
VDs	Virtual IDs
WASA	Web Application Security Audit

Glossary of Terms

Aadhaar-enabled Payment Systems (AePS): A bank-led payment model operated by National Payments Corporation of India (NPCI) that allows individuals to conduct basic financial transactions, including cash withdrawal, balance enquiry and fund transfers, using their Aadhaar number and biometric authentication at a Point of Sale (PoS) or micro-ATM device. In Direct Benefit Transfer (DBT) schemes, it enables last-mile cash access for beneficiaries who do not possess debit cards or smartphones, typically through Business Correspondents.

Aadhaar Payment Bridge System (APBS): A payment infrastructure developed by NPCI that routes DBT disbursements from government accounts directly to beneficiaries' bank accounts using their Aadhaar number as the primary identifier, rather than account number and IFSC. APBS works in conjunction with the NPCI Mapper to resolve the Aadhaar number to the linked bank account, enabling centralised, scheme-agnostic benefit transfers.

Aadhaar Data Vault (ADV): The Aadhaar Data Vault is a secure, centralised and dedicated storage system for Aadhaar numbers for entities that store Aadhaar numbers, including Authentication User Agencies (AUAs)/e-KYC User Agencies (KUAs)/sub-AUAs and organisations that collect Aadhaar numbers for internal identification purposes such as attendance management and Provident Fund (PF) linking. The Aadhaar numbers are encrypted for storage. The ADV is aimed at reducing the Aadhaar footprint in organisational systems, thus lowering the risk of unauthorised access by enforcing a standard architecture.

NPCI Mapper: A central directory operated by the NPCI, mapping individual Aadhaar numbers to the beneficiary's bank account.

Aadhaar seeding and NPCI Mapper: Process for linking and mapping beneficiaries' Aadhaar numbers to their bank accounts through the NPCI Mapper to facilitate Aadhaar-based authentication and Direct Benefit Transfers (DBT). Under the process, beneficiaries submit a signed/consented seeding request at their bank branch. The bank verifies the beneficiary's details, links their Aadhaar in the core banking system and submits a mapper-update file to NPCI through its central/IT team. NPCI processes the file and returns a response. The bank must resolve failures and confirm mapper activation. Only when mapper status is active do Aadhaar-addressed DBT credits route to that bank. For grievances (e.g., Aadhaar showing in the Core Banking System but not in the NPCI Mapper), customers must escalate via the bank, since NPCI does not modify records on its own.

Business Correspondents (BCs): Retail agents engaged by banks to provide basic banking and financial services on behalf of the bank in areas where opening a physical branch may not be viable. BCs support last-mile delivery of services such as account opening, cash deposits and withdrawals, remittances, and DBT payments, particularly in underserved and rural areas.

BC Network Managers (BCNMs): Entities engaged by banks to manage and supervise networks of BCs. BCNMs support banks in functions such as onboarding, training, monitoring, technology enablement, cash management and operational oversight of BC agents to ensure efficient last-mile delivery of banking and financial services.

Management Information Systems (MIS): Digital systems used to collect, process, manage and report information to support programme implementation, monitoring, decision-making and administrative functions. In the context of DBT and financial inclusion, MIS platforms enable the tracking of beneficiary data, transactions, fund flows and service delivery outcomes.

National Automated Clearing House (NACH): A web-based solution implemented by NPCI to facilitate interbank, high-volume electronic transactions that are repetitive and periodic.

Public Financial Management System (PFMS): The central orchestration platform for DBT payments, under the Controller General of Accounts, responsible for facilitating, overseeing and maintaining digital records of the interface between schemes and banks. It acts as both the payment gateway and the accounting backbone of DBT transactions.

Tokenisation: The generation of a Unique Identification (UID) token by the Unique Identification Authority of India (UIDAI) when a user successfully authenticates through their UID or virtual ID, which is stored by the agency or provider in their customer records.

Virtual ID (VID): A 16-digit number that can be used by individuals rather than their 12-digit Aadhaar number and can be changed by the users at will – the Aadhaar UID can only be reconstructed using the VID by the UIDAI.

A Paradigmatic Shift in Public Service Delivery: Inclusive, Efficient and Secure DPI

1. Introduction

Public service delivery has transformed significantly in the past few decades, with governments worldwide progressively embracing digital technologies to improve efficiency, transparency and access to public services. This digital transformation has evolved from the digitisation of individual services to the development of shared digital infrastructure.

Broadly, the first phase of this transition, commonly described as e-governance or e-government, focused on moving existing administrative processes online through mechanisms such as digital service portals, electronic records management systems and web-based information platforms.^{1,2} While these developments yielded considerable gains, they did not fundamentally transform how public services were organised and delivered.³ As a result, many e-government initiatives produced fragmented digital ecosystems with limited interoperability that mirrored existing bureaucratic silos, requiring citizens to navigate multiple platforms, maintain different credentials and repeatedly submit the same information. Experiences in countries such as the United Kingdom and Nigeria demonstrated the costs of this approach, where overlapping identity systems generated significant inefficiencies, including duplication and administrative burdens.^{4,5} These limitations highlighted the need for a more integrated model.

Digital Public Infrastructure (DPI) emerged as a response to these challenges. Rather than digitising individual services, DPI establishes shared, interoperable and reusable digital foundations that can support a wide range of public and private applications.⁶ DPI comprises foundational systems – digital identity, payments and data exchange that can be leveraged across sectors and use cases.⁷

The shift from e-governance to DPI represents a move from service-specific digitisation to infrastructure-led transformation. By providing common digital building blocks, DPI reduces duplication, enables interoperability and fosters innovation by enabling stakeholders like governments, the private sector, philanthropies and transnational organisations to build

¹ OECD. (2003). *The e-government imperative*. OECD Publishing. <https://doi.org/10.1787/9789264101197-en>

² Heeks, R. (2006). *Implementing and managing eGovernment: An international text*. Sage.

³ Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New public management is dead — long live digital-era governance. *Journal of Public Administration Research and Theory*, 16(3), 467–494. <https://doi.org/10.1093/jopart/mui057>

⁴ National Audit Office. (2019). *Investigation into verify*. Cabinet Office. <https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf>

⁵ Collaboration on International ICT Policy for East and Southern Africa. (2022). *Ecosystem approach to digital identification enrolment: Assessing the opportunities and risks in Nigeria*. CIPESA. <https://cipesa.org/wp-content/files/Ecosystem-Approach-to-Digital-Identification-Enrolment-Assessing-the-Opportunities-and-Risks-in-Nigeria-Report.pdf>

⁶ United Nations Development Programme. (n.d.). *Digital public infrastructure*. <https://www.undp.org/digital/digital-public-infrastructure>

⁷ Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is 'public' about DPI?* (IIPP Working Paper Series No. 2024-05). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05>

services on top of shared infrastructure.⁸ Notably, DPI also redefines the role of the state. DPI enables governments to serve as stewards of foundational infrastructure, responsible for ensuring interoperability, security, trust and equitable access while enabling broader ecosystem participation, instead of solely being a provider of digital services.⁹ Thus, DPI is more than a technological upgrade; it constitutes a new paradigm that seeks to create public value through shared digital foundations, collaborative innovation and integrated service delivery at scale.

This report examines DPI as a vehicle for accessible and inclusive, efficient and secure public service delivery by assessing how DPI performs across these dimensions, particularly in welfare distribution and healthcare delivery; identifies strategies to address gaps in design, implementation and governance; and draws broader lessons relevant to DPI adoption. To achieve this, we have developed an original evaluative framework for DPI in public service delivery, applied it to two case studies – India’s Direct Benefit Transfer (DBT) programme and the Ayushman Bharat Digital Mission (ABDM) – each examined alongside Australia’s parallel systems for welfare delivery and healthcare provisioning to derive actionable policy recommendations.

The case studies were chosen to encapsulate different relationships between DPI and service delivery. DBT is best understood as a use case – a programme that leverages existing foundational DPI layers, principally Aadhaar-linked identity and payments, to disburse welfare entitlements directly to beneficiaries. ABDM, by contrast, represents a sectoral DPI, through a dedicated identity layer (the health ID), a registry of facilities and providers, and interoperability standards for electronic health records that other healthcare applications can build upon. Fundamentally, both systems operate at a national scale, rely on foundational DPI layers and face similar challenges to ensuring inclusion for diverse populations, improving efficiencies, and maintaining robust security. However, the differences in maturity, service delivery contexts, technical and governance architectures and the enabling ecosystem demonstrate that DPI in public service delivery needs to be adapted for different sectors and institutional environments.

We conducted a systematic review of secondary literature, spanning academic literature, policy reports, government documents and publications by multilateral institutions, coupled with stakeholder engagement through consultations and interviews with government officials, civil society organisations, private sector representatives and ecosystem participants in both India and Australia, across institutions handling DPI design, implementation and oversight across welfare distribution and healthcare. Two stakeholder workshops were held

⁸ Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is ‘public’ about DPI?* (IIPP Working Paper Series No. 2024-05). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05>

⁹ Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is ‘public’ about DPI?* (IIPP Working Paper Series No. 2024-05). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05>

in India, focusing on digital health and DBT.^{10,11} A feedback conference held in Australia was also a central part of this research, bringing together implementers, practitioners, ecosystem participants and civil society actors to discuss their work and experiences in the ecosystem, validate emerging findings and solicit feedback on the report.

India was selected for this report because of its status as the most mature large-scale DPI ecosystem globally. Its foundational digital infrastructure comprising Aadhaar (identity), UPI (payment) and the Account Aggregator framework (data exchange) collectively represent the most extensive deployment of interoperable DPI for public service delivery globally. India's experience demonstrates how foundational DPIs can be deployed at population scale to strengthen public service delivery in a large and diverse country. Australia was selected for its complementary qualities: a developed governance model characterised by strong data protection frameworks, independent regulatory oversight and a mature digital infrastructure for welfare administration and healthcare. The different development contexts, governance traditions and stages of DPI maturity enable a comparative analysis that yields context-specific lessons and cross-cutting insights that can apply to other countries considering DPI adoption.

This report is organised into five chapters. This introduction establishes the context and rationale for the study, addresses what DPI is as well as its core building blocks, examines the role of DPI as a paradigmatic shift in public service delivery and provides a brief overview of India's and Australia's digital public delivery systems. Chapter 2 examines DPI within the three pillars of the Public Service Delivery Framework: Accessibility and Inclusivity, Efficiency, and Security. Chapters 3 and 4 apply the framework to welfare distribution through DBT in India and social payments in Australia (Chapter 3) and to healthcare provisioning through the ABDM in India and My Health Record in Australia (Chapter 4). Each chapter examines system design, implementation and outcomes and draws comparative lessons across the two countries. Chapter 5 synthesises the findings and observations from both case studies into cross-cutting recommendations for DPI technical design and governance, addressing themes of inclusion, efficiency and security, aimed towards countries that may be considering adopting DPI for public service delivery.

1.1 What is DPI?

While DPI has emerged as a central concept in the global development discourse, it does not yet have a universally agreed-upon definition. Table 1 lists some definitions of DPI used in various institutions and contexts.

¹⁰ Gupta, S., & Aggarwal, M. (2026). *Outcome document: Workshop on transformation of health systems through digital public infrastructure* (ICRIER Report No. 26-r-12). Indian Council for Research on International Economic Relations. <https://icrier.org/pdf/Transformation-of-Health-Systems-through-Digital-Public-Infrastructure.pdf>

¹¹ Kale, S., V S, K., Jain, N., & Aggarwal, M. (2026). *Outcome document: Workshop on digital public infrastructure and public service delivery | Inclusion. Efficiency. Security*. Indian Council for Research on International Economic Relations. <https://icrier.org/publications/outcome-document-workshop-on-digital-public-infrastructure-and-public-service-delivery-inclusion-efficiency-security/>

Table 1: Select Definitions of DPI

Source	Definition
G20 Digital Economy Working Group (2023), G20 India Presidency¹²	A set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and/or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms.
World Bank ID4D (2023)¹³	The foundational digital platforms, including institutional and legal frameworks, that underpin society-wide functions and services. This typically includes platforms for identification and authentication (as well as trust services such as e-signatures and verifiable credentials), data exchange, and payments.
World Bank White Paper (2025)¹⁴	Foundational, digital building blocks designed for the public benefit
UNDP¹⁵	A set of foundational digital systems that forms the backbone of modern societies. DPI enables secure and seamless interactions between people, businesses and governments.
OECD (2024)¹⁶	Shared digital systems that are secure and interoperable and that can support the inclusive delivery of and access to public and private services across society.
OECD extended formulation cited in World Bank White Paper (2024)¹⁷	Common, foundational digital systems that enable the delivery of services in the digital age. Elements of DPI can be developed by the public or private sector, or co-developed to benefit the delivery and access to services across both sectors, and eventually across borders. DPI needs to be standards-based and re-usable.
Digital Public Goods Alliance (2022)¹⁸	Refers to solutions and systems that enable the effective provision of essential society-wide functions and services in the public and private sectors. • This includes but is not limited to digital forms of ID and verification, civil registration, payment (digital transactions and money transfers), data exchange, and information systems (including sector-specific, i.e., health or education). • A country's digital public infrastructure may include implementations of multiple proprietary and/or open-source solutions (including digital public goods).
UCL IIPP / Eaves & Rao (2025)¹⁹	Digital Public Infrastructure (DPI) is an emerging concept in public administration and digital governance, referring to shared digital systems that support service delivery, foster innovation, and enable social and economic development.

Source: Compiled by authors

Despite variations in terminology and scope, DPI is widely understood as foundational digital systems that are open, interoperable and shared and enable service delivery at scale.

¹² G20 Digital Economy Working Group. (2023). *G20 framework for systems of digital public infrastructure*. G20 India Presidency. <https://g7g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary>

¹³ World Bank. (2023). *Global workshop on digital public infrastructure: Accelerating action*. ID4D. <https://id4d.worldbank.org/node/2113>

¹⁴ Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A. (2025). *Digital public infrastructure and development: A World Bank Group approach* (Digital Transformation White Paper, Vol. 1). World Bank. <https://openknowledge.worldbank.org/entities/publication/cca2963e-27bf-4dbb-aa5a-24a0ffc92ed9>

¹⁵ United Nations Development Programme. (n.d.). *Digital public infrastructure*. <https://www.undp.org/digital/digital-public-infrastructure>

¹⁶ OECD. (2024). *Digital public infrastructure for digital governments* (OECD Public Governance Policy Papers, No. 68). OECD Publishing. <https://doi.org/10.1787/ff525dc8-e>

¹⁷ Clark, J., Marin, G., Ardic Alper, O. P., & Galicia Rabadan, G. A. (2025). *Digital public infrastructure and development: A World Bank Group approach* (Digital Transformation White Paper, Vol. 1). World Bank. <https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf>

¹⁸ Digital Public Goods Alliance. (2022). *Unpacking concepts & definitions – digital public infrastructure, building blocks, and their relation to digital public goods*. <https://www.digitalpublicgoods.net/blog/unpacking-concepts-definitions-digital-public-infrastructure-building-blocks-and-their-relation-to-digital-public-goods>

¹⁹ Eaves, D., & Rao, K. (2025). *Digital public infrastructure: A framework for conceptualisation and measurement* (IIPP Working Paper 2025-01). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/wp2025-01>

It functions as shared infrastructure that can be leveraged across sectors and use cases and serves as the digital layer beneath applications, enabling ecosystem participants to build and deliver services on common foundations rather than through isolated systems.^{20,21} DPI extends beyond just technology to serve as a socio-technical system that combines digital infrastructure with the institutional mechanisms necessary for its effective operation, such as governance measures, legal frameworks and technical standards. There is widespread agreement that DPI serves as an enabling layer for the delivery of public and private services and contributes to wider objectives such as inclusion, innovation, economic development and public value creation.

1.2 DPI in Public Service Delivery

Historically, public service delivery has been hindered by the high costs associated with large-scale beneficiary identification, authentication and reliable benefit transfer, with conventional paper-based and early e-government systems suffering from several inefficiencies and leakages.²² DPI addresses these structural barriers by providing interoperable foundations for identity, payments and data exchange. Interactions between these layers can support a different model of public service delivery, with the State establishing shared digital foundations that can be leveraged by multiple services and can allow new services to be launched rapidly without rebuilding foundational infrastructure. It also reduces marginal costs and facilitates population-scale delivery, which was previously administratively unfeasible.²³ Research conducted after the COVID-19 pandemic highlighted that nations with robust DPI deployed emergency transfers more rapidly than those with fragmented systems.²⁴ Global institutions like the G20, United Nations Development Programme (UNDP) and World Bank have identified DPI as a critical enabler of inclusive service delivery, resulting in increased interest in DPI adoption, particularly in the Global South.^{25,26,27}

Adopting DPI for public service delivery can provide an evaluative context for DPI. Public services are a necessity for the populations that depend on them. System failures have a

²⁰ G20 Digital Economy Working Group. (2023). *G20 framework for systems of digital public infrastructure*. G20 India Presidency. <https://g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary>

²¹ OECD. (2024). *Digital public infrastructure for digital governments* (OECD Public Governance Policy Papers, No. 68). OECD Publishing. <https://doi.org/10.1787/ff525dc8-en>

²² Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106(10), 2895–2929. <https://doi.org/10.1257/aer.20141346>

²³ Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is 'public' about DPI?* (IIPP Working Paper Series No. 2024-05). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05>

²⁴ Marskell, J., Marin, G., & Varghese, M. (2023). Digital public infrastructure: Transforming service delivery across sectors. In World Bank, *Digital progress and trends report 2023* (pp. 67–84). World Bank. <https://doi.org/10.1596/978-1-4648-2049-6>

²⁵ G20 Digital Economy Working Group. (2023). *G20 framework for systems of digital public infrastructure*. G20 India Presidency. <https://g20-documents.org/database/document/2023-g20-india-sherpa-track-digital-economy-ministers-ministers-language-g20-digital-economy-ministers-meeting-outcome-document-and-chair-summary>

²⁶ United Nations Development Programme. (2023). *The human and economic impact of digital public infrastructure*. <https://www.undp.org/sites/g/files/zskgke326/files/2023-07/undp-the-human-and-economic-impact-of-digital-public-infrastructure-final.pdf>

²⁷ World Bank. (2024). *Digital progress and trends report 2023*. World Bank. <https://doi.org/10.1596/978-1-4648-2049-6>

severe impact on equity – from authentication errors to design choices that can disadvantage certain groups – and disproportionately affect vulnerable groups, potentially jeopardising access to fundamental needs such as food security and healthcare. The application of DPI in this space also requires robust governance and accountability measures, such as transparency, redressal, oversight and data protection, since it involves the exercise of state power over certain rights. Deploying DPI for public service delivery requires the utilisation of shared foundations across diverse high-stakes domains, such as linking identity to health records or welfare payments, and demonstrates whether the infrastructure is truly foundational, reusable and scalable.

Digital identity forms the foundational layer by establishing a unique, verifiable identifier that can be used across multiple services and contexts. India's Aadhaar system and Australia's MyID enable beneficiary identification and authentication, facilitate seamless access to multiple services without duplication and allow linking records for payments while ensuring privacy and user control.

Digital payments infrastructure forms the second layer by enabling instant, low-cost electronic transfer of funds between individuals, businesses, and the government. India's Unified Payments Interface (UPI), launched in 2016, provides an open architecture that allows any bank or payment service provider to build on its foundations and is being leveraged within ABDM to streamline payments processing at healthcare facilities.^{28,29,30} The integration of Aadhaar-linked bank accounts through the Jan Dhan, Aadhaar, and Mobile (JAM) trinity has enabled Direct Benefit Transfers to bypass intermediaries and reach beneficiaries directly,³¹ and Australia's New Payments Platform, launched in 2018, provides a comparable real-time payments infrastructure integrated with Services Australia's social payments systems.³²

Data exchange infrastructure forms the third layer by enabling secure, consent-based sharing of personal data across service providers. India's Account Aggregator, drawing from the Data Empowerment and Protection Architecture (DEPA) framework, allows individuals to share financial data with lenders and other providers through a standardised interface, without requiring those providers to store the data, reducing information asymmetries and expanding access to credit for those with limited collateral.³³ This consent-based model has been adopted in ABDM for health information exchange. Similarly, Australia operates My Health Record, a centralised national platform for health data exchange.

²⁸ National Payments Corporation of India. (2024). *UPI product statistics*. <https://www.npci.org.in/product/upi/product-statistics>

²⁹ Alonso, C., Bhojwani, T., Hanedar, E., Prihardini, D., Uña, G., & Zhabaska, K. (2023). *Stacking up the benefits: Lessons from India's digital journey* (IMF Working Paper No. 2023/078). International Monetary Fund. <https://www.imf.org/en/Publications/WP/Issues/2023/04/05/Stacking-Up-the-Benefits-Lessons-from-Indias-Digital-Journey-532092>

³⁰ National Health Authority. (n.d.). *Scan & Pay*. Ayushman Bharat Digital Mission. <https://abdm.gov.in/scan-pay>

³¹ Ministry of Finance, Government of India. (2021). *Economic survey 2020–21* (Vol. 1, pp. 78–82). Government of India Press.

³² Ministry of Finance, Government of India. (2021). *Economic survey 2020–21* (Vol. 1, pp. 78–82). Government of India Press.

³³ Sahamati. (2024). *Data capital: Unlocking formal finance for a billion Indians*. <https://sahamati.org.in/wp-content/uploads/2024/12/Sahamati-Annual-Report-2024.pdf>

DPI's potential hinges on building mechanisms capable of identifying and addressing system failures and enabling and sustaining public trust through transparency and accountability, as exemplified by the highlighted case studies.

2. Evaluative Framework for DPI in Public Service Delivery

The global diffusion of DPI has outpaced the development of comprehensive evaluative frameworks for assessing whether DPI delivers on its promise of accessible, inclusive, efficient and secure public services. Without such frameworks, policymakers risk entrenching patterns of digital exclusion, embedding inefficiencies in public systems under the guise of digitisation and causing security and privacy risks that undermine public trust.

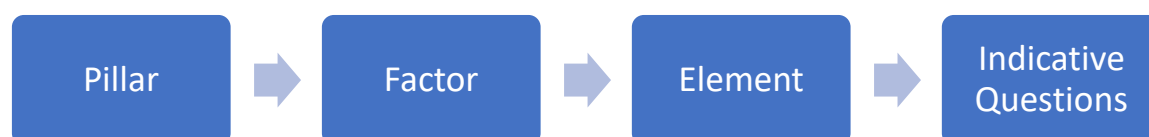
This report presents a framework to evaluate and guide DPI implementation in public service delivery. The framework serves a dual purpose: it is evaluative and diagnostic as it provides a structured lens through which to assess how existing DPI implementations perform, identifies gaps and risks and helps generate recommendations to remedy those gaps; and it is normative as it articulates that DPI should be grounded in principles of inclusivity, efficiency and security.

The framework organises DPI assessment around three interdependent pillars: Accessibility and Inclusivity, Efficiency, and Security, where each pillar corresponds to a distinct but interrelated dimension of DPI performance.

Framework Overview

The DPI Assessment Framework is organised hierarchically, moving from high-level pillars to granular indicative questions. Each of the three pillars – Accessibility and Inclusivity, Efficiency, and Security – is divided into Factors, which are further divided into elements, which are then operationalised through indicative questions to translate abstract principles into concrete assessment criteria. Figure 1 illustrates the hierarchical structure of the framework.

Figure 1: Structure of the Framework



Source: Authors' own

This hierarchical structure enables high-level strategic assessment at the pillar level and detailed operational evaluation at the indicator level. The framework has been designed for broad cross-country applicability and can be applied to assess and evaluate DPI in public service delivery across implementation use cases and in diverse governance contexts.

In the first pillar, **Accessibility and Inclusivity**, accessibility refers to enabling overarching non-discriminatory, equal access to DPI systems for different users, while inclusivity is a broader term that recognises and addresses, through targeted approaches, barriers to participation for diverse socioeconomic groups.³⁴ Thus, this pillar aims to ensure that infrastructure reaches all populations, particularly historically marginalised groups. The second pillar, **Efficiency**, captures DPI's promise to reduce costs, streamline service delivery and enable innovation through shared infrastructure. The third pillar, **Security**, includes privacy, cybersecurity, fraud prevention and governance mechanisms that protect individuals, build trust and maintain system integrity.

Table 2 presents an overview of the framework, outlining the deconstruction of each Pillar into Factors and subsequently into Elements. The complete framework with indicative questions for each element is provided in Annexure 1.

Table 2: Overview of DPI for the Public Service Delivery Assessment Framework

Pillar	Factor	Elements
1. Accessibility and Inclusivity	1.1 User Diversity & Reach	1.1.1. Gender Inclusion 1.1.2. Disability Access 1.1.3. Inclusion of Migrants and Mobile Populations 1.1.4. Socioeconomic & Literacy Inclusion 1.1.5. Geographic Coverage
	1.2 Access Mechanism	1.2.1 Digital & Assisted Channels 1.2.2 Inclusion Efforts to Engage Minority/Marginalised Groups
	1.3 Feedback/Redressal	1.3.1 Grievance Redressal Channels 1.3.2 Digital & Financial Literacy Support
2. Efficiency	2.1 Optimising the Process	2.1.1 Improving/Simplifying the Process 2.1.2 Improvements in Time & Speed
	2.2 Cost Efficiency	2.2.1 For the System 2.2.2 For Users
	2.3 System Capacity	2.3.1 Scalability & Resilience
	2.4 Innovation	2.4.1 Interoperability & Integration 2.4.2 Multiple Use Cases 2.4.3 Innovation & Public-Private Partnerships
3. Security	3.1 Privacy & Data Protection	3.1.1 Privacy by Design 3.1.2 Data Storage & Processing 3.1.3 User Control & Rights
	3.2 Cybersecurity	3.2.1 Governance 3.2.2 Identify 3.2.3 Protect 3.2.4 Detect 3.2.5 Respond 3.2.6 Recover
	3.3 Fraud & Risk Management	3.3.1 Authentication & Verification 3.3.2 Fraud Monitoring & Response

³⁴ The terms 'inclusivity' and 'inclusion' are used to refer to both dimensions in this report.

		3.3.3 Grievance Mechanisms for Security Breaches
	3.4 Governance & Compliance	3.4.1 Legal & Regulatory Compliance 3.4.2 Transparency & Accountability 3.4.3 User Trust & Communication 3.4.4 Algorithmic Accountability

Source: Authors' own

The Framework provides standardised assessment categories and recognises that an appropriate balance among the three pillars can vary across contexts depending on governance capacity, digital infrastructure maturity and policy priorities. Thus, the framework captures internalised trade-offs and unintended consequences in the DPI system. The Framework is not structured to produce aggregate scores that can obscure underlying problems; instead, it is designed to accommodate emerging DPI capabilities and evolving governance challenges while maintaining analytical consistency.

Notably, while the three pillars are analytically distinct, they are not independent of each other. Some assessment criteria can span multiple pillars. For instance, governance appears within the security pillar but also has direct implications on efficiency and accessibility. Similarly, authentication design is assessed under fraud and risk management, but authentication failures also pose accessibility concerns. The hierarchical categories in the framework should be treated as structured analytical tools rather than fixed silos and aim to address how findings in one pillar affect assessments in others.

2.1 Pillar 1: Accessibility and Inclusivity

This pillar recognises that DPI's technical capabilities do not automatically translate into desirable outcomes. It also includes DPI's fundamental promise of extending public services to populations that have previously been excluded. Accessibility and inclusivity are foundational to DPI legitimacy: systems that exclude marginalised groups or create barriers to access fail to deliver on the purpose that justifies their deployment.³⁵ Digital systems that reproduce or amplify exclusion result in two-tier service delivery, where digitally connected populations benefit while marginalised groups face new barriers. Digital exclusion, in turn, can generate downstream costs in the form of increased manual interventions, redressal burdens and loss of public trust.

Pillar 1 comprises three Factors, viz., User Diversity and Reach, Access Mechanism, and Feedback and Redressal.

³⁵ United Nations Development Programme. (2023). *Accelerating the SDGs through digital public infrastructure: A compendium of the potential of digital public infrastructure*. <https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure>

User Diversity and Reach

This factor examines whether DPI systems achieve coverage across demographic, socioeconomic and geographic dimensions. It also recognises that universal coverage in aggregate statistics may mask the systematic exclusion of specific groups. Addressing this requires disaggregated analysis to reveal disparities.

1.1 User Diversity and Reach

Element 1.1.1 Gender Inclusion

Element 1.1.2 Disability Access

Element 1.1.3 Inclusion of Migrants and Mobile Populations

Element 1.1.4 Socioeconomic and Literacy Inclusion

Element 1.1.5 Geographic Coverage

Gender Inclusion in DPI design requires careful attention to registration processes to ensure women can enrol independently. It also demands authentication modalities to account for asymmetric device access and the deployment of user interfaces to support diverse literacy levels and languages.

Disability Access is another consideration. Inaccessible authentication mechanisms increase both the risk of exclusion and the risk of security failure for people with disabilities, leading to situations where those most at risk are least able to protect themselves.³⁶ Accessible DPI design requires compliance with recognised accessibility standards, provision of alternative authentication modalities and systematic usability testing with diverse user groups.

Inclusion of Migrants and Mobile Populations assesses whether DPI systems enable the portability of identity credentials and entitlements across administrative boundaries to accommodate the needs of internal migrants, seasonal workers and other mobile populations. It considers policy issues such as the existence of pathways to update registered addresses without triggering re-enrolment or loss of benefit history and the availability of alternative registration mechanisms for those without stable addresses.

Socioeconomic and Literacy Inclusion examines whether DPI reaches groups that are simultaneously the most dependent on public services and the most vulnerable to digital exclusion, such as low-income populations and those with limited digital literacy. Inclusive design strategies include multilingual interfaces in vernacular languages, simplified user journeys, assisted registration and hybrid service delivery models that provide non-digital fallback options.

³⁶ Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, 3(5), Article 346. <https://doi.org/10.1007/s42979-022-01239-1>

Geographic Coverage assesses whether DPI infrastructure and services effectively reach rural, remote, tribal and underserved areas and if they receive equivalent service quality, connectivity and support for offline infrastructure.

Access Mechanism

This factor recognises that not all users can or should be required to interact with digital systems to access public services. It evaluates the channels and modalities through which users interact with DPI, assessing whether DPI systems provide multiple channels for enrolment, authentication and service delivery.

1.2 Access Mechanism

Element 1.2.1 Digital and Assisted Channels

Element 1.2.2 Inclusion Efforts to Engage Minority and Marginalised Groups

Digital and Assisted Channels examine the availability and quality of both self-service digital channels and assisted channels, including in-person service centres, telephone helplines and community intermediaries. Hybrid models that combine digital efficiency with human assistance are particularly important for populations with limited digital capacity or persistent authentication difficulties.

Inclusion Efforts to Engage Minority and Marginalised Groups recognises that inclusion requires deliberate outreach. These efforts also assess whether DPI systems go beyond passive non-discrimination and proactively identify and address the barriers facing ethnic, linguistic, religious, caste-based and other marginalised communities.

Feedback and Redressal

This factor highlights the significance of effective grievance redressal mechanisms by recognising that even well-designed systems generate errors and exclusions. It also examines whether DPI systems provide accessible mechanisms for users to report problems, seek assistance and obtain remedies when access fails.

1.3 Feedback and Redressal

Element 1.3.1 Grievance Redressal Channels

Element 1.3.2 Digital and Financial Literacy Support

Grievance Redressal Channels examines the availability of responsive redressal mechanisms, which determines whether system failures are corrected or become entrenched exclusion patterns. This element assesses if multi-channel, multi-language grievance mechanisms are accessible to non-digital users and persons with disabilities, with defined response timelines and transparent escalation procedures.

Digital and Financial Literacy Support recognises that accessibility requires ongoing institutional support and capacity-building efforts and evaluates whether users receive sustained support to build the digital and financial literacy needed to use DPI effectively. It covers literacy programmes, availability of support in local and vernacular languages and non-text formats and the ability of programmes to build capacity for independent use rather than nurture perpetual dependence on intermediaries.

2.2 Pillar 2: Efficiency

This pillar evaluates whether DPI delivers on its promise of reduced transaction costs, faster service delivery and administrative simplification while building system capacity for scale and resilience. Efficiency extends beyond cost reduction to encompass process improvement, scalability and innovation. This pillar assesses whether DPI delivers measurable improvements in service delivery speed, cost-effectiveness, scalability and innovation. Capacity building is a vital factor of this pillar; the efficiency gains enabled by DPI can only be sustained if the institutional, human and technical capacities required to operate, maintain and improve systems are embedded at all levels of implementation.

The pillar comprises four Factors; Optimising the Process, Cost Efficiency, System Capacity, and Innovation.

Optimising the Process

This factor maintains that efficiency gains must translate to improved user experiences rather than remaining administrative performance metrics. It examines whether DPI is streamlining service delivery workflows, simplifying bureaucratic procedures, accelerating service delivery and improving user experience.

2.1 Optimising the Process
Element 2.1.1 Improving and Simplifying the Process
Element 2.1.2 Improvements in Time and Speed

Improving and Simplifying the Process recognises that poorly designed digital systems can replicate or amplify bureaucratic complexity and that simplification must be evaluated from user perspectives. It assesses whether DPI implementation results in substantive process simplification, such as reduction in procedural steps, elimination of redundant documentation, automation of routine verification decisions and improvement in citizen experience.

Improvements in Time and Speed evaluates whether DPI reduces service delivery time across the full-service lifecycle, from application processing to identity verification to decision-making and benefit disbursement.

Cost Efficiency

This factor evaluates whether DPI reduces costs for both service providers and users.

2.2 Cost Efficiency

Element 2.2.1 For the System

Element 2.2.2 For Users

Cost Efficiency for the System examines whether DPI reduces the cost-of-service delivery for government, including administrative, personnel, infrastructure and transaction costs, through cost per service transaction, whether documented savings are available and methodologically credible, how the cost structure of DPI compares to the systems it replaces and reductions in fraud or leakage.

Cost Efficiency for Users evaluates whether DPI reduces the costs borne by users for accessing services, including travel and documentation costs, formal cost to access the service (if any), informal payments to intermediaries and opportunity costs such as wages lost due to time away from work.

System Capacity

This factor assesses whether DPI infrastructure can accommodate growth in users and transactions while maintaining performance and resilience during crises or disruptions.

2.3 System Capacity

Element 2.3.1 Scalability and Resilience

Scalability and Resilience examines whether DPI can expand to population scale and maintain functionality during crises; its ability to handle increased loads and maintain service during disruptions; and whether capacity-planning processes exist to anticipate future growth. At population scale, DPI systems become critical infrastructure, and failure can have cascading effects across welfare delivery, financial services and public administration.

Innovation

This factor captures DPI's potential to enable new services and business models through shared infrastructure, foster interoperability and support public-private collaboration.

2.4 Innovation

Element 2.4.1 Interoperability and Integration

Element 2.4.2: Multiple Use Cases

Element 2.4.3: Innovation and Public-Private Partnerships

Interoperability and Integration assesses whether DPI modules can be combined and reused across services and whether systems adhere to open standards that enable third-party innovation and cross-agency integration. Assessing whether interoperability is achieved across the complete ecosystem of public and private actors can help examine whether identity, payment and data platforms work seamlessly across agencies and third parties.

Multiple Use Cases evaluates whether the DPI system can support diverse service delivery contexts beyond its primary application, identify spillover effects (if any) and explore how the effects are measured and attributed to DPI design choices.

Innovation and Public-Private Partnerships examines whether DPI has enabled private-sector participation while maintaining public purpose and user protection.

2.3 Pillar 3: Security

This pillar assesses privacy protections, cybersecurity measures, fraud prevention and governance safeguards against surveillance, discrimination and misuse of personal data. Security is essential for building trustworthiness in DPI. The stakes are also higher at population scale as failures can have cascading effects, compromising sensitive personal data records, disrupting essential services and eroding public trust in digital government.

The pillar comprises four Factors; Privacy and Data Protection, Cybersecurity, Fraud and Risk Management, and Governance and Compliance.

Privacy and Data Protection

This factor examines whether DPI embeds privacy protections throughout the data lifecycle and respects user rights.

3.1 Privacy and Data Protection
Element 3.1.1 Privacy by Design
Element 3.1.2 Data Storage and Processing
Element 3.1.3 User Control and Rights

Privacy by Design recognises that privacy protections need to be built into DPI architecture from the beginning. Privacy-by-design principles include data minimisation, purpose limitation and technical safeguards such as encryption, pseudonymisation and anonymisation.³⁷ These principles must simultaneously be embedded in policy frameworks and reflected in technical architecture. This factor considers whether DPI systems conduct privacy impact assessments and implement their findings. It also provides for clear and granular consent processes as well as clearly defined, monitored and enforced data retention and deletion standards.

³⁷ OECD. (2024). *Digital public infrastructure for digital governments*. OECD Public Governance Policy Papers. OECD Publishing. <https://doi.org/10.1787/ff525dc8-en>

Data Storage and Processing evaluates the security of data storage and processing throughout the data lifecycle. The baseline requirements for credible data security include encryption of data, rules about access and clear standards for partner and third-party data-handling that are contractually enforced through regular independent audits.

User Control and Rights examines whether individuals can access, correct and control their personal data and if consent for data use can be granted and withdrawn in a meaningful and accessible manner, including by those with low digital literacy.

Cybersecurity

This factor evaluates technical and organisational measures to protect DPI systems against cyberattacks, data breaches and unauthorised access. This Factor requires ongoing vigilance and adaptation. Additionally, it requires organisational and governance capability to be distributed across the full lifecycle of system design, operation and incident management.

3.2 Cybersecurity
Element 3.2.1 Governance
Element 3.2.2 Identify
Element 3.2.3 Protect
Element 3.2.4 Detect
Element 3.2.5 Respond
Element 3.2.6 Recover

Governance examines whether DPI has clear cybersecurity leadership and organisational accountability structures and whether cyber risk has been integrated into risk management strategies. Effective cybersecurity requires designated leadership, clearly defined roles and responsibilities, formal risk acceptance processes and continuous reassessment during operation. It also requires that cybersecurity responsibilities shared with suppliers, partners and participants are documented, communicated and subject to independent assurance.

Identify assesses whether DPI operators or implementors have a clear understanding of assets, vulnerabilities and the threat landscape. It includes considerations such as whether confidentiality, integrity and availability requirements are recorded for all components; security risks across the full technology stack are identified and regularly updated; and interdependencies between components are identified so as to understand and document the cascading impact of system compromise on connected systems.

Protect evaluates the technical and procedural controls in place to prevent cyber incidents. It emphasises the secure-by-design and secure-by-default principles outlined in the Australian Cyber Security Strategy³⁸ and provides that systems should be designed with security embedded from the outset and that default configurations should provide adequate

³⁸ Australian Government Department of Home Affairs. (2023). *2023–2030 Australian cyber security strategy*. <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy>

protection without requiring user action. It further requires data to be encrypted and authenticated at rest and in transit using approved algorithms and protocols to protect confidentiality and integrity.

Detect examines whether DPI operators have the capability to identify cyber incidents promptly and includes considerations such as whether security-related event logs are centrally gathered, securely stored and promptly analysed; changes to security configurations are logged and monitored; cybersecurity events are analysed to identify potential incidents enabling rapid response; and cybersecurity event detection capabilities are regularly evaluated for effectiveness and continuously refined.

Respond evaluates if DPI operators can effectively manage cyber incidents, including containing, eradicating and recovering data. Assessments include whether formal incident response, business continuity and disaster recovery plans exist and are regularly exercised to support continued operations during an incident; compensating and communicating with affected stakeholders is undertaken; and lessons from incidents are documented and fed into improvements.

Recover evaluates whether DPI operators can securely resume normal business operations following a cybersecurity incident. Assessments include whether systems undergo formal assurance activities following an incident to verify they are secure and capable of supporting resumption before being returned to service; and whether residual security risks, including any inherited or shared risks that persist after the incident, are formally accepted prior to the resumption of normal business operations.

Fraud and Risk Management

This Factor evaluates measures to prevent, detect and respond to fraudulent access, identity theft and unauthorised use of DPI systems.

3.3 Fraud and Risk Management
Element 3.3.1 Authentication and Verification
Element 3.3.2 Fraud Monitoring and Response
Element 3.3.3 Grievance Mechanisms for Security Breaches

Authentication and Verification assesses the strength, reliability and effectiveness of identity verification mechanisms that allow access to DPI-enabled services, including the availability of alternative authentication methods and de-duplication measures. Providing accessible alternatives for users who cannot comply with the standard requirements of the predominant identity verification mechanisms is a key concern. For example, it is necessary to provide alternative identity verification mechanisms to people with degraded biometrics, such as the elderly, manual labourers or persons with disabilities, who may not be able to use the predominant method of a fingerprint scan.

Fraud Monitoring and Response evaluates the processes to detect and respond to fraudulent transactions, unauthorised access and identity misuse.

Grievance Mechanisms for Security Breaches examines whether users have accessible channels to report security incidents, identity theft or fraud and if they receive timely support and remediation, which may include identity restoration and benefit reinstatement.

Governance and Compliance

This factor evaluates if DPI operates within robust legal and regulatory frameworks, has adequate transparency and accountability mechanisms and maintains user trust.

3.4 Governance and Compliance
Element 3.4.1 Legal and Regulatory Compliance
Element 3.4.2 Transparency and Accountability
Element 3.4.3 User Trust and Communication
Element 3.4.4 Algorithmic Accountability

Legal and Regulatory Compliance examines whether the DPI system is backed by a legislative framework and complies with applicable data protection, privacy, cybersecurity and sector-specific regulatory requirements, such as guardrails for third-party compliance and regular compliance audits by credible, independent reviewers.

Transparency and Accountability evaluates if the governance of DPI is transparent, subject to independent oversight and accountable to users and the public. It includes regular disclosures of audit findings, independent review reports and the establishment of clear lines of accountability for data stewardship and incident management.

User Trust and Communication examines whether DPI operators cultivate public trust by clearly communicating with users about data use, security measures and user rights. It also examines whether ecosystem trust is built through clear articulation of the obligations and liabilities of participants.

Algorithmic Accountability assesses whether automated decision-making processes embedded in DPI systems are transparent, contestable and subject to independent oversight. As DPI systems increasingly incorporate algorithmic decision-making in their operations, transparency requirements for automated processes, user rights to explanation and contestation of algorithmic decisions, mandatory fairness and bias audits, and human review mechanisms for consequential decisions have to be included as core accountability requirements.

2.4 Using the Framework for Holistic Assessment of DPI

The three pillars are mutually reinforcing requirements, and any assessment that treats them in isolation will systematically misrepresent a DPI system's performance. Their interconnections result in concrete design and governance choices that can simultaneously

affect outcomes across all three domains. An excessive emphasis on any one pillar without adequate consideration of the others can weaken overall system performance. For instance, stringent authentication requirements or complex access controls may improve security but can erode inclusivity by locking out vulnerable and underserved populations who cannot meet standard verification thresholds. Conversely, prioritising efficient data exchange without commensurate security safeguards may increase the risks of fraud, identity theft and data breaches, ultimately undermining public trust. Similarly, efficiency gains that overlook barriers faced by digitally excluded users may improve administrative performance while reinforcing existing divides.

Literature from multilateral institutions and international ecosystem participants also agrees that accessibility, efficiency and security must be pursued together rather than sequenced or traded off against one another.^{39,40,41,42} Thus, managing these trade-offs is a key governance challenge in the design and implementation of DPI-enabled public services.

In chapters 3 and 4, we apply the framework to assess India's and Australia's DPI implementations across welfare distribution and healthcare provisioning, respectively. We examine both country contexts against all three pillars, drawing out trade-offs, design choices and governance arrangements that shape whether DPI delivers on its promise of accessible, inclusive and secure public service delivery. Instead of exhaustively evaluating each DPI use case against all indicative questions of the framework, we draw on select factors and elements of the case studies appropriate to their respective service delivery contexts for a broader assessment.

3. Case Study: Direct Benefit Transfer

3.1 Introduction

India's Direct Benefit Transfer (DBT) system is a globally recognised model for digital government-to-person (G2P) payments within a Digital Public Infrastructure (DPI) framework. By enabling direct transfers of subsidies, pensions, wages and income support into beneficiaries' bank accounts, DBT has reconfigured welfare delivery from distortionary, regressive and intermediary-driven systems to a standardised, digitally mediated system.^{43,44} Instead of providing welfare delivery benefits through subsidised prices, it transfers benefits directly to individuals, improving targeting, transparency and efficiency.

³⁹ OECD. (2024). *Digital public infrastructure for digital governments*. OECD Public Governance Policy Papers. OECD Publishing. <https://doi.org/10.1787/ff525dc8-en>

⁴⁰ World Bank. (2023). *Global workshop on digital public infrastructure: Accelerating action*. ID4D. <https://id4d.worldbank.org/node/2113>

⁴¹ United Nations Development Programme. (2023). *Accelerating the SDGs through digital public infrastructure: A compendium of the potential of digital public infrastructure*. <https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure>

⁴² Global Partnership for Financial Inclusion. (2023). *G20 policy recommendations for advancing financial inclusion and productivity gains through digital public infrastructure*. World Bank. <https://documents1.worldbank.org/curated/en/099092023121016458/pdf/P178703046f82d07c0bbc60b5e474ea7841.pdf>

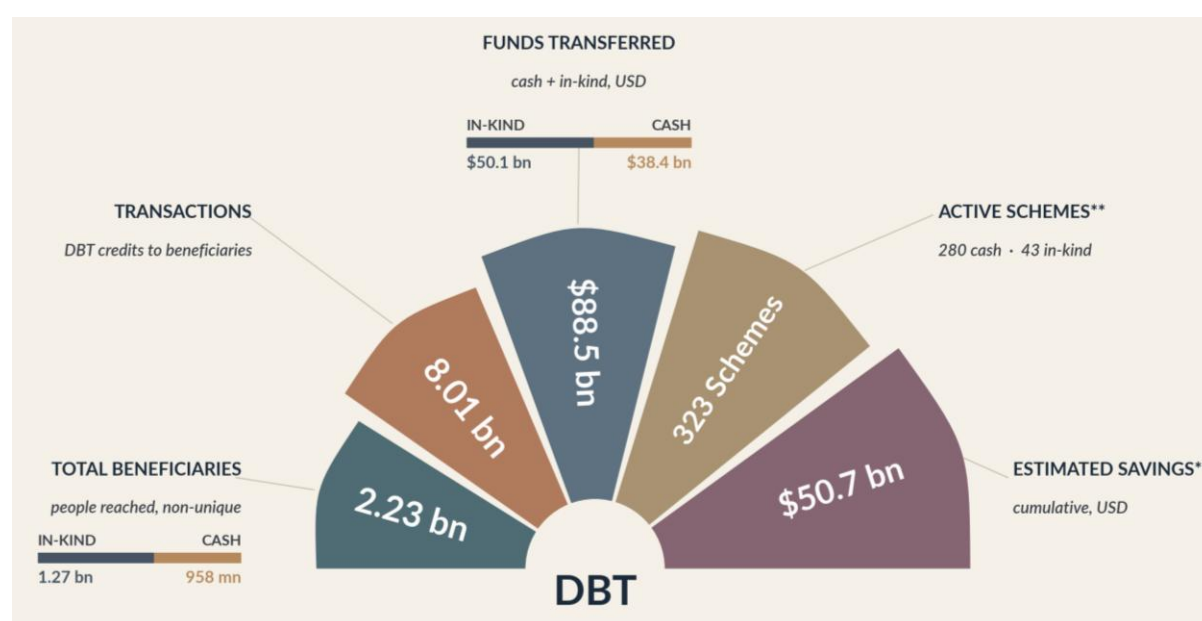
⁴³ Joy, J. (2018). A critical analysis of direct benefit transfer in India. *Indian Journal of Economics and Development*, 6(8), 1-7.

⁴⁴ Tiwari, S. K., & Kamila, A. (2023, June). Direct Benefit Transfer in India: A global role model. *Yojana: A Development Monthly*.

While DBT draws conceptually from global experiences with cash transfer programmes, such as Brazil’s Bolsa Família and Mexico’s Progres a/Oportunidades, India’s model reflects a distinct institutional trajectory. Rather than being a standalone welfare reform, DBT emerged as a systemic response to inefficiencies in a large and complex welfare architecture characterised by fragmented beneficiary databases, leakages, delays and weak monitoring.⁴⁵ The system, led by the Nandan Nilekani Task Force (2011),⁴⁶ laid the foundation for an integrated approach combining digital identity, banking infrastructure and interoperable payment systems.

Launched in 2013 and subsequently scaled nationwide, DBT’s expansion has been enabled by the Jan Dhan–Aadhaar–Mobile (JAM) trinity.⁴⁷ As of June 2026, DBT spans 323 central and over 2,500 state schemes (Figure 2), covering sectors such as food subsidies, Liquefied Petroleum Gas (LPG), agriculture, employment, pensions and scholarships, and serving nearly two billion beneficiaries annually.

Figure 2: Status of India’s DBT System as of 2026



Sources: Authors’ own, based on the [DBT Bharat Portal](#)

Notes: All figures relate to FY 2025-26 unless otherwise stated. USD equivalents at INR 85 = 1 USD (FY 2025-26 average). Beneficiary count is non-unique – the same person may receive support under multiple schemes. The figure was designed using Claude AI.

*Cumulative efficiency gains reported up to March 2024 – savings from PAHAL, PDS, MGNREGA and other DBT-enabled schemes.

**Count of active DBT schemes as of FY 2026-27.

⁴⁵ Joy, J. (2018). A critical analysis of direct benefit transfer in India. *Indian Journal of Economics and Development*, 6(8), 1-7.

⁴⁶ Choi, J., & Xavier, J. (2021). Digitalization of public service delivery in Asia. *Asian Productivity Organization*, 1(1), 1-184.

⁴⁷ Joy, J. (2018). A critical analysis of direct benefit transfer in India. *Indian Journal of Economics and Development*, 6(8), 1-7.

Beyond scale, DBT represents a shift in the design logic of welfare delivery. At its core, DBT operates as a layered digital infrastructure integrating identity (Aadhaar), public financial management system (PFMS), interoperable payment systems (managed by the National Payment Corporation of India (NPCI)), rails such as the Aadhaar Payment Bridge System (APBS) and National Automated Clearing House (NACH)), and last-mile access channels (bank accounts, Business Correspondents (BCs), Aadhaar-enabled Payment Systems (AePS)). This architecture aligns with key DPI principles while addressing longstanding challenges in welfare delivery (Table 3).

Table 3: DBT Architecture Through the Lens of DPI Principles

Traditional System Challenges	DPI Principle	DBT Infrastructure	How DPI Improves Welfare Delivery
Fragmented beneficiary databases and duplicate records across schemes	Unique digital identity	Aadhaar-based identification	Reduces duplication and improves targeting accuracy
Manual payment processes and delays in fund disbursement	Digitalisation and scalability	PFMS	Standardises and scales payment authorisation and processing
Lack of coordination between banks and government departments	Interoperable payment infrastructure	NPCI payment rails (APB, NACH)	Allows seamless routing and settlement of payments
Leakages and diversion of funds through intermediaries	Transparency and auditability	PFMS digital audit trail and electronic transfers	Improves traceability of funds and reduces corruption
Limited banking access in rural areas	Financial inclusion and last-mile access	Jan Dhan accounts, BCs, AePS	Expands access to banking and enables cash-out services

Source: Authors' analysis based on secondary literature and stakeholder insights

International institutions have described India's DBT system as a "logistical marvel," particularly highlighting its role in delivering large-scale support during crises such as the COVID-19 pandemic.⁴⁸ However, its outcomes have been neither uniform nor unambiguous. While digitalisation has improved efficiency and traceability, it has also introduced new challenges related to data accuracy, authentication reliability, last-mile access and governance.

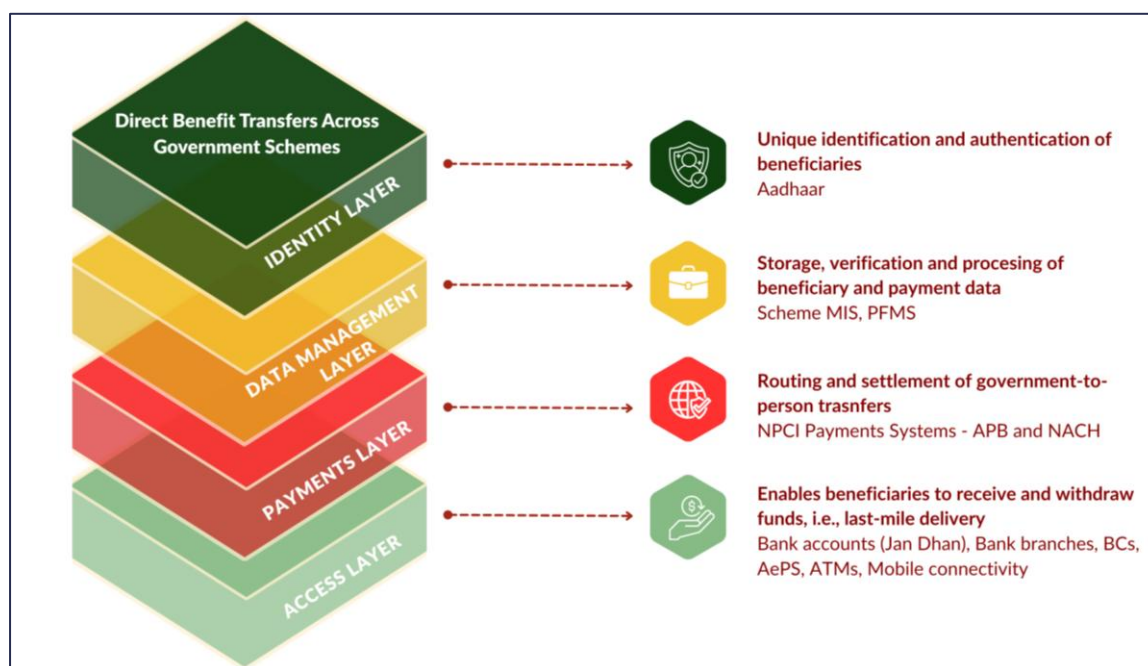
DBT therefore embodies both the promise and complexity of DPI-led welfare systems, enabling scale and efficiency. This chapter analyses DBT through this lens, examining how its technical architecture, governance frameworks and implementation choices shape outcomes across three key dimensions: inclusion and access, efficiency, and security. The chapter also benchmarks India's DBT system with Australia's welfare delivery system and provides recommendations.

⁴⁸ Tiwari, S. K., & Kamila, A. (2023, June). Direct Benefit Transfer in India: A global role model. *Yojana: A Development Monthly*.

3.2 Technical Architecture

From a broader perspective, DBT can be understood as a layered DPI integrating four interdependent layers – identity, data management, payments infrastructure and last-mile financial access – to deliver welfare benefits at scale (Figure 3).

Figure 3: DBT as a Layered DPI Stack



Source: Authors' own representation based on secondary literature

Notes: Scheme MIS is Scheme Management Information System; PFMS is Public Financial Management System; NPCI is National Payments Corporation of India; APB is Aadhaar Payment Bridge; NACH is National Automated Clearing House; BC is Banking Correspondent; AePS is Aadhaar Enabled Payment System

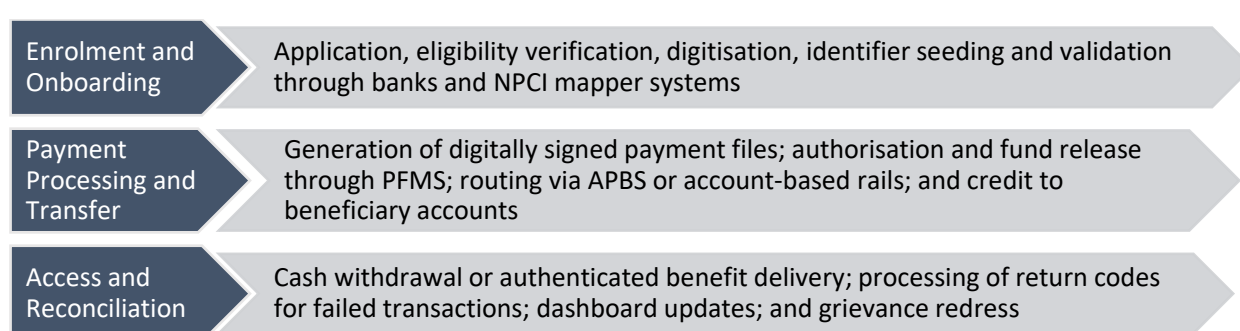
At the foundation is the identity layer, namely Aadhaar, which provides a unique digital identity for beneficiaries and supports authentication and de-duplication across welfare databases. With over 142 crore Aadhaar enrolments as of 2025,⁴⁹ this layer establishes a common identification framework that underpins beneficiary targeting and verification. The data and transaction management layer comprises scheme-specific Management Information Systems (MIS) and the PFMS. Together, these systems maintain beneficiary records, verify eligibility, authorise welfare payments and generate digital payment instructions.⁵⁰

⁴⁹ Unique Identification Authority of India. (n.d.). *Unique Identification Authority of India*. <https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html>

⁵⁰ Government of India, DBT Mission. (2013). *Report on Direct Benefit Transfer*. Cabinet Secretariat. <https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf>

The interoperable payments layer, operated primarily by the NPCI, enables the routing and settlement of transfers across the banking system through platforms such as APBS and NACH. By using Aadhaar or bank account details as financial addresses, these systems standardise and scale bulk payment processing across schemes and institutions. Finally, the access and financial inclusion layer ensures that beneficiaries can receive and withdraw funds through a range of channels, including bank accounts, BCs, AePS, ATMs and assisted digital interfaces. This layer is critical in translating digital transfers into actual access to funds, particularly in rural and underserved areas.⁵¹ Together, these layers form a standardised, end-to-end pipeline for welfare delivery, replacing fragmented and manual processes with an integrated and auditable system (Figure 4).

Figure 4: End-to-End Process Flow of DBT



Source: Authors' own, based on secondary literature

The effectiveness of this architecture depends on a set of technical and operational conditions. Accurate seeding of Aadhaar with bank accounts and the integrity of NPCI mapper systems are critical for correct payment routing. The reliability of authentication mechanisms, particularly biometric systems, directly affects beneficiaries' ability to access funds. Further, the system relies on interoperability across multiple platforms, including scheme databases, PFMS and banking networks, where mismatches or delays can result in transaction failures. Failures at any stage can propagate across layers, affecting the overall effectiveness of service delivery. Stakeholder consultations highlighted that the effectiveness of the architecture also depends on the reliability of local administrative processes, connectivity infrastructure and human intermediaries involved in enrolment, updating and reconciliation activities.

3.3 Governance of the DBT Stack

The DBT architecture operates as a multi-layered governance framework that determines how identity is verified, payments are authorised and routed and accountability is enforced across the welfare delivery chain. This governance structure can be understood across three interlinked layers: constitutional and legal safeguards governing digital identity, regulatory institutions overseeing infrastructure and operational arrangements involving public and

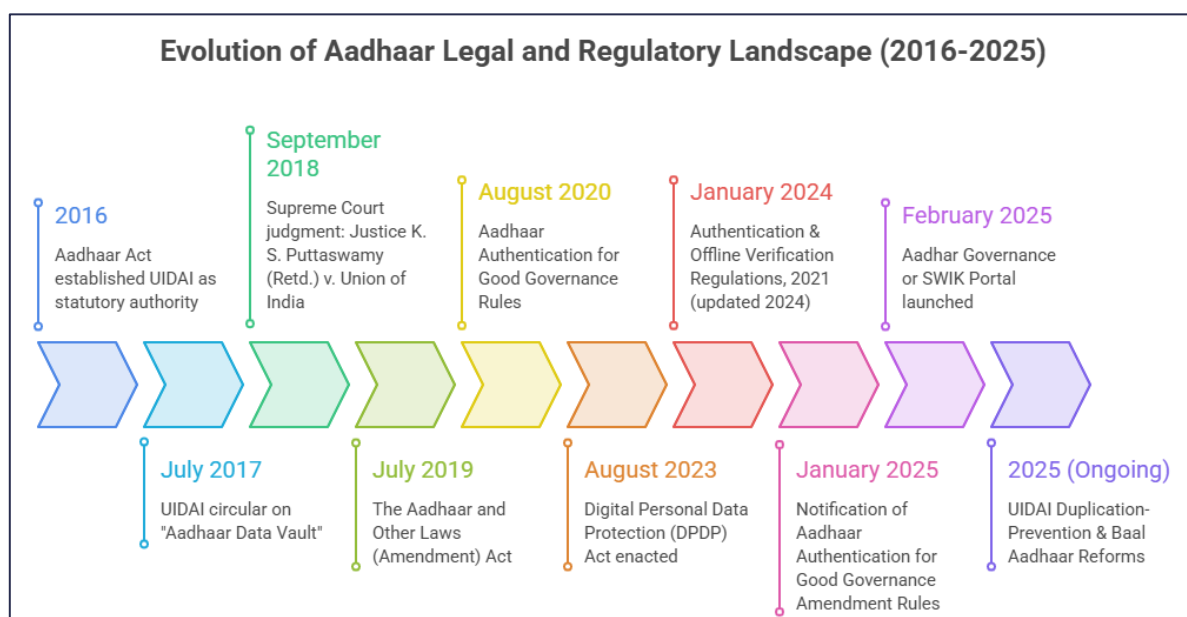
⁵¹ Government of India, DBT Mission. (n.d.). *Guidelines for State DBT Cell*. Cabinet Secretariat. <https://pmksy.gov.in/pdflinks/DBTCellGuidelinesforState.pdf>

private actors. These layers operationalise the Governance & Compliance factor of the evaluation framework by shaping the elements related to legal and regulatory compliance, transparency, accountability and institutional oversight of digital service delivery.

3.3.1 Constitutional Governance of Digital Identity: Aadhaar's Legal Evolution

The evolution of DBT, often described as DBT 2.0 and DBT 3.0, has been intertwined with the evolution of Aadhaar as a “near” national digital identity infrastructure, shaped by judicial scrutiny and legislative reform (Figure 5). While the earlier phases of DBT primarily focused on digitising beneficiary identification and streamlining fund transfers, the DBT 3.0 framework envisions a more integrated and proactive welfare architecture. By enabling interoperability across administrative databases, these models seek to reduce repetitive documentation, automate eligibility verification and enable welfare systems to proactively deliver or modify benefits when beneficiaries record life events or changes in eligibility. At the same time, the expanding role of Aadhaar and interconnected state databases has raised broader concerns regarding privacy, proportionality, data sharing, profiling and the permissible scope of state-led digital identity systems, as indicated by stakeholders.

Figure 5: Evolution of Aadhaar in India: Key Milestones



Source: Authors' own, based on secondary literature

The Aadhaar Act, 2016⁵² provided statutory backing to the system and established the Unique Identification Authority of India (UIDAI) as the central regulator. However, the scope of Aadhaar was subsequently narrowed by the Supreme Court in 2018,⁵³ which upheld its use

⁵² Government of India. (2016). *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (as amended)*. Unique Identification Authority of India. https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

⁵³ Supreme Court Observer. (n.d.). *Constitutionality of Aadhaar: Justice K.S. Puttaswamy v. Union of India (plain English summary)*. <https://www.scoobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/>

for targeted welfare delivery while striking down provisions that enabled unrestricted private-sector access. The Supreme Court emphasised that digital identity systems must operate within constitutional safeguards, particularly the principles of proportionality and informational privacy.

Subsequent regulatory reforms have sought to operationalise these safeguards. The Aadhaar Authentication and Offline Verification Regulations (2021, updated in 2024)⁵⁴ introduced alternatives to biometric authentication, including one-time password (OTP)-based and offline verification mechanisms. More broadly, DBT operates within a legal framework comprising identity governance under the Aadhaar Act and data protection under the Digital Personal Data Protection (DPDP) Act, 2023.⁵⁵

While implementing agencies function as data fiduciaries under this framework, welfare delivery is typically grounded in statutory mandate rather than meaningful consent. In practice, beneficiaries often have limited ability to refuse Aadhaar-linked authentication or data processing without risking disruptions in access to welfare entitlements. Therefore, consent within DBT systems operates under conditions of unequal bargaining power, where participation in digital systems is closely tied to access to essential public services.

The DPDP Act grants the Central Government broad exemption powers in relation to the processing of personal data. Section 17 enables notified instrumentalities of the state to be exempt from significant parts of the Act on grounds including national security, public order and sovereignty. Critics have argued that these provisions create wide executive discretion and may dilute privacy safeguards by exempting certain public authorities from obligations relating to notice, consent, purpose limitation and accountability.⁵⁶

3.3.2 Regulatory Governance of the DBT Ecosystem

The operational functioning of DBT is governed through a network of specialised institutions that oversee different components of the delivery chain. At the policy level, the DBT Mission, housed in the Cabinet Secretariat, provides strategic direction, develops standardisation protocols and coordinates implementation across ministries. Line ministries maintain scheme-specific beneficiary databases and generate payment instructions, while state DBT cells support implementation and reporting at the sub-national level.⁵⁷

At the identity layer, UIDAI regulates Aadhaar enrolment, authentication and data security (see section 3.6). At the financial layer, PFMS, operated by the Controller General of Accounts,

⁵⁴ Unique Identification Authority of India. (2021). *The Aadhaar (Authentication and Offline Verification) Regulations, 2021*. https://uidai.gov.in/images/The_Aadhaar_Authentication_and_Offline_Verifications_Regulations_2021.pdf

⁵⁵ Ministry of Electronics and Information Technology. (2023). *The Digital Personal Data Protection Act, 2023*. Government of India. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

⁵⁶ <https://internetfreedom.in/iffs-public-brief-on-the-digital-personal-data-protection-framework/>

⁵⁷ Comptroller and Auditor General of India. (2021). *Organisation and management of Direct Benefit Transfer* (Chapter VII). Government of India.

functions as the central platform for authorising and tracking welfare payments.⁵⁸ Once authorised, payments are routed through NPCI-managed payment systems, which operate under the regulatory oversight of the Reserve Bank of India (RBI).⁵⁹ This institutional architecture creates a distributed system of checks and balances. By allocating oversight across multiple institutions, the DBT framework reduces the risk of unilateral control but also requires seamless coordination across actors.

3.3.3 Private-Sector Participation in the DBT Ecosystem

Although DBT is a state-led welfare system, its implementation relies extensively on private-sector participation, particularly in the banking, payments and technology layers. Banks, both public and private, play a central role in maintaining beneficiary accounts and processing transactions. They also deploy BCs and associated network managers, often private entities or fintech firms, to deliver last-mile banking services in areas with limited formal infrastructure. These agents facilitate withdrawals and authentication-based transactions through micro-ATMs and AePS-enabled devices.⁶⁰ Private technology providers also supply and maintain authentication infrastructure, including biometric devices, point-of-sale (PoS) systems used in schemes such as the Aadhaar-enabled Public Distribution System (AePDS)⁶¹ and software systems used in welfare delivery. As a result, DBT functions as a hybrid public-private system, where public institutions define rules and standards while private actors provide operational capacity.

The scope of private-sector participation within the DBT ecosystem is also shaped by the regulatory framework governing Aadhaar-based authentication. Since authentication services underpin several DBT processes, judicial and legislative developments concerning Aadhaar have influenced the extent to which private entities can participate in identity verification and related service delivery functions. The Supreme Court's 2018 judgment restricted unrestricted private use of Aadhaar authentication, citing risks of profiling and commercial exploitation. Subsequent reforms, including the Aadhaar (Amendment) Act, 2019⁶² and the SWIK (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025,⁶³ reintroduced limited private participation under controlled conditions, establishing an approval-based framework for access to authentication services.

⁵⁸ Choi, J., & Xavier, J. (2021). Digitalization of public service delivery in Asia. *Asian Productivity Organization*, 1(1), 1-184.

⁵⁹ Government of India, DBT Mission. (n.d.). *Guidelines for State DBT Cell*. Cabinet Secretariat. <https://pmksy.gov.in/pdflinks/DBTCellGuidelinesforState.pdf>

⁶⁰ Government of India, DBT Mission. (2013). *Report on Direct Benefit Transfer*. Cabinet Secretariat. <https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf>

⁶¹ Government of India, DBT Mission. (n.d.). *Success story*. <https://dbtbharat.gov.in/success-story/view?id=NQ==>

⁶² Government of India. (2019). *The Aadhaar and Other Laws (Amendment) Act, 2019*. Unique Identification Authority of India. https://uidai.gov.in/images/news/Amendment_Act_2019.pdf

⁶³ Press Information Bureau. (2025, January 31). *Notification of Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Amendment Rules, 2025*. Government of India. <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2098223®=3&lang=2>

Box 1: The Debate on Private Access to Aadhaar

The Debate on Private Access to Aadhaar

The reintroduction of controlled private access to Aadhaar authentication has revived longstanding concerns regarding the expanding use of identity-linked verification beyond welfare delivery. While policymakers argue that providing the private sector regulated access to the Aadhaar infrastructure through the SWIK Rules, 2025, can improve service delivery across sectors such as finance, e-commerce and healthcare, critics caution that expanding authentication capabilities risks function creep, profiling and the gradual normalisation of pervasive identity verification.⁶⁴

In practice, the boundary between public and private use has already been evolving. Selected financial service providers have been permitted to use Aadhaar-based verification under regulatory oversight following the rollout of the Aadhaar (Amendment) Act, 2019, while platforms such as DigiLocker have enabled private firms such as HyperVerge to build digital identity verification and know-your-customer services on top of public digital infrastructure.⁶⁵

The SWIK Rules, 2025, formalise this shift by introducing a structured approval process for private-sector entities involving relevant ministries, UIDAI and the Ministry of Electronics and Information Technology.⁶⁶ While these safeguards introduce procedural controls such as purpose limitation and regulatory oversight, concerns remain regarding the adequacy of mechanisms ensuring user control, data retention limits and long-term implications for the constitutional principles established in the Aadhaar judgement. The debate therefore reflects a broader governance challenge: balancing innovation and efficiency gains from private participation with the need to preserve privacy, accountability and the limited use of digital identity systems.⁶⁷

3.4 Accessibility and Inclusivity

DBT is designed to expand welfare access by enabling direct transfers across a wide range of schemes targeting diverse beneficiary groups, including the elderly, women, children, persons with disabilities, farmers and low-income households. By replacing cash-based delivery with account-based transfers linked to digital identity, DBT seeks to reduce intermediaries, improve targeting and enhance transparency. However, inclusion in DBT depends on whether beneficiaries can successfully navigate each stage of the delivery chain. Exclusion therefore arises not from a single point of failure but from cumulative frictions across access, identification, payment processing and last-mile delivery.

⁶⁴ Pandey, K. (2025, February 3). *Private companies and Aadhaar authentication*. MediaNama. <https://www.medianama.com/2025/02/223-private-companies-aadhaar-authentication/>

⁶⁵ Huynh, H. (2025, August 18). Public infrastructure and private surveillance in India's Aadhaar system. *TechPolicy.Press*. <https://www.techpolicy.press/public-infrastructure-and-private-surveillance-in-indias-aadhaar-system/>

⁶⁶ Agrawal, A. (2025, February 28). Portal unveiled to help private entities apply for Aadhaar authentication. *Hindustan Times*. <https://www.hindustantimes.com/india-news/portal-unveiled-to-help-pvt-entities-apply-for-aadhaar-authentication-101740682753298.html>

⁶⁷ Fox Mandal & Associates. (2025). Aadhaar authentication for private entities: Navigating the 2025 amendment. *Lexology*. <https://www.lexology.com/library/detail.aspx?g=a0dc6f01-463d-407e-b45d-720b489e3661>

Drawing on the accessibility and inclusivity dimension of the evaluation framework, the following sub-sections examine factors such as user diversity and reach through gender, disability, migrant and mobile populations; access mechanisms through digital and assisted channels; grievance redressal and feedback systems; and inclusion-exclusion trade-offs inherent in DPI-enabled welfare delivery.

3.4.1 Entry and Access Stage

The JAM architecture has played a critical role in lowering barriers to financial inclusion.⁶⁸ The rapid expansion of bank accounts under the Pradhan Mantri Jan Dhan Yojana (PMJDY), supported by simplified know-your-customer (KYC) norms and digital identity, has enabled the large-scale onboarding of previously unbanked populations.⁶⁹ This expansion has also substantially reduced gender gaps in financial access. According to the Global Findex Database 2025, India has achieved near-universal account ownership among adults, with no statistically significant differences across gender.⁷⁰

However, account ownership does not automatically translate into effective access. Social norms, mobility constraints, intra-household control over finances and limited financial and digital literacy, particularly among women, can restrict independent use of accounts.⁷¹ Similarly, access to mobile phones and familiarity with digital interfaces remains uneven, affecting the ability of beneficiaries to interact with digital systems.⁷²

Evidence from scheme-level implementation further highlights the role of information asymmetries in shaping access outcomes. While awareness of flagship programmes such as Ayushman Bharat (PM-JAY) exceeds 70% overall, it remains significantly lower among poorer households. Even among those who are aware, enrolment and utilisation rates remain limited to only about 16%, suggesting that the most vulnerable beneficiaries are often the least informed and face additional barriers in accessing welfare schemes.⁷³

While digital systems lower entry barriers, they introduce new requirements in terms of identity verification, account usability and interaction with digital interfaces. Emerging voice-based and vernacular technologies may help address literacy and language barriers.⁷⁴ Reflecting this shift, UIDAI is developing more user-centric Aadhaar interfaces, signalling a

⁶⁸ Umesh, R., & Nagaraju, Y. (2025). Role of Direct Benefit Transfer schemes in promoting financial inclusiveness among rural beneficiaries: An assessment study. *International Journal for Research Trends and Innovation*, 10(8).

⁶⁹ Choi, J., & Xavier, J. (2021). Digitalization of public service delivery in Asia. *Asian Productivity Organization*, 1(1), 1-184.

⁷⁰ Klapper, L., Singer, D., Starita, L., & Norris, A. (2025). *The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy*. World Bank. doi:10.1596/978-1-4648-2204-9.

⁷¹ Field, E., Pande, R., Rigol, N., Schaner, S., & Troyer Moore, C. (2021). On her own account: How strengthening women's financial control impacts labor supply and gender norms. *American Economic Review*, 111(7), 2342-2375. <https://doi.org/10.1257/aer.20200705>

⁷² Stakeholder insights.

⁷³ Bhatnagar, A., Chhabra, S., Manchanda, N., & Smith, O. (2022). *PM-JAY awareness, enrolment and targeting: Evidence from a national household survey* (PM-JAY Policy Brief No. 11). National Health Authority.

⁷⁴ Malik, P., Jain, N., Kanwar, S., Das, B. & Dhadwal, S. (2025). *AI markets and competition in India*. ICRIER. <https://icrier.org/pdf/AI-Markets-and-Competition-in-India.pdf>

move towards improving accessibility and usability.⁷⁵ However, the effectiveness of such innovations depends on their deployment and last-mile adoption.

3.4.2 Beneficiary Identification and Eligibility

Inclusion in DBT depends on whether eligible individuals are accurately identified and included within scheme databases. While Aadhaar has enabled large-scale standardisation of beneficiary records and improved traceability across schemes,⁷⁶ identification outcomes continue to be shaped by the design and quality of underlying targeting frameworks.⁷⁷

Most welfare schemes rely on large-scale surveys such as the Socio Economic and Caste Census,⁷⁸ which classify households based on deprivation indicators. However, these lists are static and are not updated in real time or regularly.⁷⁹ Targeting outcomes are further influenced by the political economy. Discretionary practices in beneficiary selection, reliance on outdated identifiers such as below poverty line (BPL) lists and weak alignment between eligibility criteria and current socioeconomic conditions can result in the systematic exclusion of vulnerable groups, including migrants and informal workers.⁸⁰

Migrant populations face more acute challenges within welfare delivery systems. While Aadhaar itself is portable across states, eligibility for many welfare programmes continues to depend on location-specific beneficiary databases, domicile requirements or administrative records that may not adequately capture population mobility. As a result, migrants may remain excluded from welfare benefits despite possessing valid identity credentials. Initiatives such as the One Nation, One Ration Card (ONORC) have sought to address these portability constraints by enabling access to subsidised food grains across states.^{81,82} However, limited awareness and uneven implementation constrain the full portability of welfare entitlements.

⁷⁵ Stakeholder insights.

⁷⁶ Umesh, R., & Nagaraju, Y. (2025). Direct Benefit Transfer in India: Progress, challenges, and the path forward. *International Journal for Multidisciplinary research*, 7(1).

⁷⁷ Desai, S. (2024, July 15). *Rethinking social safety nets in a changing society*. Ideas for India.

<https://www.ideasforindia.in/topics/poverty-inequality/rethinking-social-safety-nets-in-a-changing-society>

⁷⁸ This includes automatic inclusion (e.g., particularly vulnerable groups), automatic exclusion (e.g., ownership of certain assets or formal employment) and a graded scoring system based on occupation, housing conditions and demographic characteristics.

⁷⁹ Comptroller and Auditor General of India. (2024). *Report No. 3 of 2024: Audit of social sector and compliance audit (SSCA)*. Government of India. https://cag.gov.in/uploads/download_audit_report/2024/Report-No.-3-of-2024_AB-SSCA_English_PDF-A-066b360783c2d56.50376374.pdf

⁸⁰ Desai, S. (2024, July 15). *Rethinking social safety nets in a changing society*. Ideas for India.

<https://www.ideasforindia.in/topics/poverty-inequality/rethinking-social-safety-nets-in-a-changing-society>

⁸¹ Roy, D., Saroj, S., Boss, R. & Pradhan, M. (2021, August 16). *PDS, National Food Security Act, and Covid-19*. Ideas for India.

<https://www.ideasforindia.in/topics/poverty-inequality/pds-national-food-security-act-and-covid-19.html>

⁸² Gupta, K., Soni, P., Rautela, K. & Srinivas, K. (2023). *Uptake, implementation, portability, and operability of the One Nation One Ration Card: A study*. (ADB Brief No. 270). Asian Development Bank. <https://www.adb.org/sites/default/files/publication/923066/adb-brief-270-one-nation-one-ration-card.pdf>

Box 2: Identity Does Not Imply Eligibility

Identity Does Not Imply Eligibility: Lessons from the Special Intensive Revision Debate

A recurring assumption in discussions on DPI is that stronger digital identity systems can, by themselves, resolve problems of access and inclusion. The Special Intensive Revision (SIR) of electoral rolls undertaken by the Election Commission of India highlighted the limits of this assumption. During the exercise, concerns emerged regarding individuals whose names were missing from or subject to verification in electoral databases despite the individuals possessing Aadhaar cards and other government-issued identity documents.⁸³

In hearing challenges to the SIR exercise, the Supreme Court reiterated an important distinction: Aadhaar may serve as a valid proof of identity, but it is not conclusive proof of citizenship.⁸⁴ More broadly, the Supreme Court reaffirmed that identity verification and eligibility determination are distinct administrative functions that rely on different databases, legal criteria and verification processes.⁸⁵

This distinction is equally relevant for DBT systems. Possessing a valid Aadhaar number may establish that a person is who they claim to be, but it does not automatically establish eligibility for a welfare scheme. Access to benefits depends on the accuracy, completeness and regular updating of programme-specific databases that determine who qualifies for a particular entitlement. As a result, individuals who possess valid identity credentials may still be excluded if their records are missing, outdated, incorrectly linked or subject to administrative verification processes. The SIR debate therefore highlights the distinction between identity, eligibility and entitlement, demonstrating that foundational identity infrastructure alone cannot eliminate the risks arising from database errors, record mismatches or administrative exclusion.

⁸³ Bhattacharya, S. (2026, April 12). Political turmoil in Indian border state as nine million lose voting rights. *BBC*. <https://www.bbc.com/news/articles/cy51gg00dezo>

⁸⁴ *Association for Democratic Reforms and Others v. Election Commission of India and Others*, W.P. (C) No. 640/2025 (Supreme Court of India May 27, 2026). <https://www.supremecourtcases.com/association-for-democratic-reforms-and-others-v-election-commission-of-india-and-others/>

⁸⁵ Times of India Desk. (2025, September 8). Bihar SIR: SC says Aadhaar proof of identity but not citizenship—what it means. *The Times of India*. <https://timesofindia.indiatimes.com/india/bihar-sir-sc-says-aadhaar-proof-of-identity-but-not-citizenship-what-it-means/articleshow/123765502.cms>

3.4.3 Payment Processing and Authentication

Once beneficiaries are enrolled, inclusion depends on the successful processing and authentication of transactions across multiple system layers. Delays in payment authorisation, routing failures, account-related issues or mismatches across systems can affect the timeliness and reliability of transfers.⁸⁶ These frictions could often lead to workarounds at the point of transaction, resulting in “adjusted transactions”.⁸⁷

While authentication systems improve traceability and reduce the possibility of manipulation of records, they also introduce new forms of exclusion. Biometric failures arising from worn fingerprints among manual labourers, poor biometric capture among elderly populations, device malfunction and connectivity constraints can prevent beneficiaries from successfully authenticating transactions.⁸⁸ This is illustrated in PM-KISAN, where mandatory e-KYC and Aadhaar-seeding requirements have disrupted the payment processing of eligible beneficiaries due to authentication failures, incomplete documentation and system readiness gaps.⁸⁹

UIDAI has introduced several fallback provisions, including OTP-based authentication, iris authentication, exception-handling mechanisms and assisted updates to reduce exclusion from biometric failures. However, the effectiveness of these safeguards often depends on mobile and network access, which remain uneven across regions.⁹⁰ Stakeholders also pointed towards ongoing technological adaptations within the Aadhaar ecosystem, including the increasing adoption of face authentication mechanisms to reduce dependency on fingerprint quality and dedicated biometric devices. Such developments reflect attempts to improve authentication reliability, particularly for populations engaged in manual labour or residing in low-resource settings.

3.4.4 Last-Mile Access: BCs, AePS and Cash-Out Infrastructure

The final stage of DBT delivery, accessing transferred funds, remains one of the most critical determinants of inclusion. The BC model supported by AePS has played a central role in extending banking services to underserved areas. Through micro-ATMs and assisted service points, BCs enable beneficiaries to withdraw cash, check balances and conduct basic

⁸⁶ Comptroller and Auditor General of India. (2024). *Report No. 3 of 2024: Audit of social sector and compliance audit (SSCA)*. Government of India. https://cag.gov.in/uploads/download_audit_report/2024/Report-No.-3-of-2024_AB-SSCA_English_PDF-A-066b360783c2d56.50376374.pdf

⁸⁷ “Adjusted transaction” means that retailers use their own or someone else’s Aadhaar number to authenticate and register sales, either during the time of the sale or after. Such “adjusted transactions” may also imply situations where a retailer registers all sales for the day using only a few Aadhaar numbers. MicroSave Consulting. (2019). *Direct Benefit Transfer in fertilizer: 4th round of concurrent evaluation – A National study*. microsave.net/wp-content/uploads/2019/03/190327_DBT-in-Fertilizer_National-Study_Published.pdf

⁸⁸ Seth, A., Gupta, A., Johri, M., Narayan, A., Kumar, N., Kumar, A., & Kumar, A. (2021, March 25). *Delivery of social protection entitlements in India: Unpacking exclusion, grievance redress, and the relevance of citizen-assistance mechanisms*. Azim Premji University.

⁸⁹ Niti Tantra. (2023). *Challenges in direct benefit transfer implementation and the way forward*. <https://nititantra.com/challenges-in-direct-benefit-transfer-implementation-and-the-way-forward/>

⁹⁰ Seth, A., Gupta, A., Johri, M., Narayan, A., Kumar, N., Kumar, A., & Kumar, A. (2021, March 25). *Delivery of social protection entitlements in India: Unpacking exclusion, grievance redress, and the relevance of citizen-assistance mechanisms*. Azim Premji University.

transactions without requiring access to formal bank branches.⁹¹ Complementary channels such as post offices and Common Service Centres (CSCs) have further expanded this access network.⁹²

However, the effectiveness of this system depends on the performance of agent networks. Constraints related to network density, liquidity availability, device functionality and connectivity can significantly affect the reliability of cash-in cash-out (CICO) services. Where BCs operate under low commissions or face cash shortages and lack training, beneficiaries may encounter irregular service, repeated transaction failures or informal charges.⁹³

Empirical evidence highlights persistent access barriers. Beneficiaries often travel long distances to reach access points, face long waiting times and make multiple visits due to transaction failures or liquidity constraints.⁹⁴ Global Findex 2021 showed that 43% of unbanked Indian adults cited distance to financial institutions as a barrier to last-mile financial access.⁹⁵ Technical failures in devices and connectivity further disrupted access.⁹⁶

Several stakeholders also noted that, in remote and low-connectivity regions, digital workflows continue to rely on manual supplementation, including offline forms, delayed uploads and intermediary-assisted verification processes. In several hard-to-reach regions, frontline implementation agencies reported that the absence of Aadhaar enrolment or incomplete identity documentation among vulnerable communities continued to delay onboarding into welfare systems.

These frictions impose substantial transaction costs on beneficiaries, which are often not captured in DBT efficiency assessments. These costs include travel expenses, time spent waiting at access points, lost wages due to repeated visits and informal fees charged by intermediaries.^{97,98} User preferences and trust play a critical role in shaping access outcomes. Despite the expansion of digital infrastructure, many beneficiaries continue to rely on cash-based transactions, reflecting concerns around reliability, ease of use and control over funds.⁹⁹ Recognising that digital infrastructure alone does not guarantee digital inclusion, policymakers have increasingly emphasised assisted service delivery through CSCs, BCs,

⁹¹ Raghavan, M. (2020, May). *Transaction failure rates in the Aadhaar-enabled payment system: Urgent issues for consideration and proposed solutions*. Dvara Research.

⁹² Government of India, DBT Mission. (2013). *Report on Direct Benefit Transfer*. Cabinet Secretariat.
<https://dbtbharat.gov.in/data/documents/REPORT-ON-DBT.pdf>

⁹³ Iyer, A. (2023). *An agent success framework – Part I: Why agent networks must offer access to reliable Cash-in Cash-out (CICO) services?* Dvara Research. <https://dvararesearch.com/an-agent-success-framework-part-i-why-agent-networks-offer-access-to-reliable-cash-in-cash-out-cico-services/>

⁹⁴ Roy, D., Saroj, S., Boss, R. & Pradhan, M. (2021, August 16). *PDS, National Food Security Act, and Covid–19*. Ideas for India.
<https://www.ideasforindia.in/topics/poverty-inequality/pds-national-food-security-act-and-covid-19.html>

⁹⁵ <https://dvararesearch.com/an-agent-success-framework-part-i-why-agent-networks-offer-access-to-reliable-cash-in-cash-out-cico-services/>

⁹⁶ Raghavan, M. (2020, May). *Transaction failure rates in the Aadhaar-enabled payment system: Urgent issues for consideration and proposed solutions*. Dvara Research.

⁹⁷ <https://rupe-india.org/aspects-no-81-82/digitalisation-in-india-the-class-agenda-part-iii/#c747bf29-f0f7-47c0-9d2b-5d774866b4ff>

⁹⁸ Comptroller and Auditor General of India. (2024). *Report No. 3 of 2024: Audit of social sector and compliance audit (SSCA)*. Government of India. https://cag.gov.in/uploads/download_audit_report/2024/Report-No.-3-of-2024_AB-SSCA_English_PDF-A-066b360783c2d56.50376374.pdf

⁹⁹ MicroSave Consulting. (2019). *Direct Benefit Transfer in fertilizer: 4th round of concurrent evaluation – A national study*. microsave.net/wp-content/uploads/2019/03/190327_DBT-in-Fertilizer_National-Study_Published.pdf

Indian Post Payments Bank (IPPB) networks and other last-mile support mechanisms. These channels are intended to bridge gaps in digital literacy, strengthen user trust and improve access for beneficiaries who may be unable or unwilling to rely exclusively on self-service digital platforms.¹⁰⁰

3.4.5 Grievance Redressal

The effectiveness of DBT systems depends not only on delivery but also on the ability of beneficiaries to resolve failures across the delivery chain. In practice, formal grievance redress mechanisms remain weak due to procedural complexity, low awareness and limited accessibility.¹⁰¹ As a result, beneficiaries often rely on informal intermediaries such as local representatives, frontline workers or civil society organisations to access information, escalate issues and navigate administrative processes.

These patterns point to structural gaps in grievance design. Local functionaries are often more accessible but lack decision-making authority, while higher-level authorities, who can resolve issues, are harder to reach. Even where institutional mechanisms exist, they are often underutilised due to complexity and low digital literacy. Fundamentally, beneficiaries frequently lack clarity on the source of failure, whether arising from authentication errors, backend processing delays or data inconsistencies, which require them to engage with multiple institutions. This shifts the burden of resolution onto users.¹⁰² Strengthening grievance systems therefore requires simplified processes, greater local-level authority, user-centric frameworks and integrated tracking across agencies.¹⁰³

3.4.6 Inclusion–Exclusion Trade-Offs

The inclusion challenges within DBT ultimately reflect broader design trade-offs embedded in digital welfare systems. Measures intended to improve targeting accuracy, reduce leakages and strengthen auditability often increase dependence on standardised databases, authentication protocols and automated decision-making systems. While these mechanisms improve scalability and administrative efficiency, they may reduce flexibility in accommodating diverse beneficiary circumstances, particularly in contexts characterised by weak documentation, infrastructural gaps and low digital capability.

These tensions are not inherent to digitalisation itself but are shaped by governance choices, implementation design and institutional capacity. The effectiveness of DBT depends not only on technological architecture but on the extent to which systems incorporate grievance resolution, local adaptability and fallback mechanisms to minimise exclusion risks across the delivery chain.

¹⁰⁰ Stakeholder insights.

¹⁰¹ Roy, D., Saroj, S., Boss, R. & Pradhan, M. (2021, August 16). *PDS, National Food Security Act, and Covid-19*. Ideas for India. <https://www.ideasforindia.in/topics/poverty-inequality/pds-national-food-security-act-and-covid-19.html>

¹⁰² Stakeholder insights.

¹⁰³ Ghosh, I. (2022, September). From digital payments to financial inclusion: The challenges ahead. *ISB Management ReThink*, 3(4).

As DBT systems increasingly use automated matching, verification and eligibility determination, the key question is not only whether a decision is technically accurate but whether it is fair, reviewable and responsive to individual circumstances. Systems should retain meaningful human discretion and accessible exception pathways, particularly where an automated outcome may interrupt an essential entitlement. Automation should reduce administrative burdens without making beneficiaries responsible for proving or correcting system errors.

3.5 Efficiency and Performance

This section examines how interoperable digital infrastructure and standardised service delivery optimise the DBT process and improve cost efficiency and system capacity. Public welfare delivery is characterised by informational asymmetries¹⁰⁴ and frictions,¹⁰⁵ where governments rely on intermediaries to identify beneficiaries and deliver benefits, which risks leakage, delay and diversion.¹⁰⁶ DBT seeks to reduce these frictions by linking transfers to authenticated identities and routing payments through standardised digital systems.¹⁰⁷

3.5.1 Fiscal and Transaction Efficiency

According to estimates, the cumulative fiscal savings from DBT schemes till March 2024 amount to roughly INR 4.31 trillion, over 50% of which has been attributed to deletion of duplicate and fake ration cards under the Public Distribution System (PDS).¹⁰⁸ A 2025 report¹⁰⁹ similarly noted that, while aggregate subsidy allocations as a share of total government expenditure declined from an average of 16% during 2009-13 to 9% in 2023-24, beneficiary coverage expanded from INR 11 crore to INR 176 crore.

A key illustration of these efficiency gains is the reform of LPG subsidies under the Direct Benefit Transfer for LPG (DBTL) scheme. Rather than eliminating in-kind provision, DBTL altered the subsidy mechanism: households purchase LPG at market prices and receive the subsidy directly in their bank accounts. This shift reduced the scope for diversion arising from the dual-price system where subsidised cylinders were previously redirected to commercial markets. The reform is estimated to have reduced subsidised household LPG sales by 46%, largely by curbing leakage and ghost consumption while generating estimated savings of USD 3–6 billion between 2015 and 2019 and improving the monitoring of subsidy delivery.¹¹⁰

¹⁰⁴ Akerlof, G. A. (1978). The economics of “tagging” as applied to the optimal income tax, welfare programs, and manpower planning. *The American Economic Review*, 68(1), 8-19.

¹⁰⁵ Duflo, E., & Banerjee, A. (2011). *Poor economics* (Vol. 619). New York: PublicAffairs.

¹⁰⁶ Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.

¹⁰⁷ Khera, R. (2019). Aadhaar: Uniquely Indian dystopia? *Economic Sociology: The European Electronic Newsletter*, 21(1), 4-12.

¹⁰⁸ Selected scheme-wise breakdown is given in Table 2.1 of Appendix 2. DBT Bharat. (n.d.). *Estimated gains: Estimated benefits/gains from DBT and other governance reforms (upto March 2024)*. <https://dbtbharat.gov.in/static-page-content/spagecont?id=18>

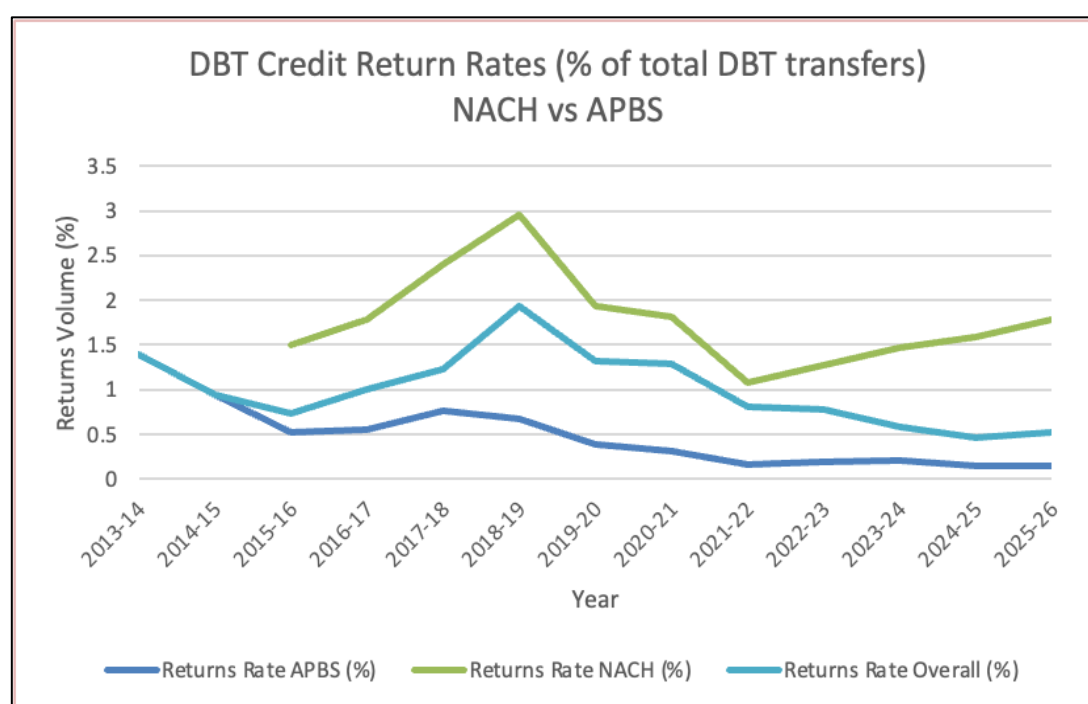
¹⁰⁹ Selected scheme-wise breakdown is given in Table 2.1 of Appendix 2. DBT Bharat. (n.d.). *Estimated gains: Estimated benefits/gains from DBT and other governance reforms (upto March 2024)*. <https://dbtbharat.gov.in/static-page-content/spagecont?id=18>

¹¹⁰ Barnwal, P. (2024). Curbing leakage in public programs: Evidence from India’s Direct Benefit Transfer policy. *American Economic Review*, 114 (12): 3812–46. DOI: 10.1257/aer.20161864

In addition to reforms in subsidy delivery mechanisms, Aadhaar-based authentication systems have strengthened administrative efficiency by improving traceability and reducing opportunities for proxy collection and manipulation of beneficiary records. At the front end, biometric and OTP-based authentication mechanisms facilitate beneficiary verification, while the introduction of ePoS devices in the PDS has enabled real-time transaction recording and monitoring.¹¹¹ These measures have optimised the benefit delivery process, improved programme integrity and helped reduce diversion of food grains by linking benefit delivery to authenticated beneficiaries.

More broadly, the increasing use of standardised payment infrastructure, particularly systems such as APBS, has enabled high-volume processing of transfers with greater consistency across schemes, boosting cost efficiency for the system. Compared to earlier account-based or manual systems (e.g., NACH), these systems have led to lower failure rates, improvements in transaction reliability and administrative scalability¹¹² (Figure 6).

Figure 6: Efficiency Gains Through Aadhaar-Authenticated Direct Benefit Transfers



Source: Authors' own, based on data from NPCI and NACH Product Statistics (March 2026)¹¹³

Notes: DBT transfers do not include LPG subsidies; Returns volume overall (%) is calculated as (Returns Volume APBS + Returns Volume NACH) * 100 / Total DBT Transfers

¹¹¹ Choi, J., & Xavier, J. (2021). Digitalization of public service delivery in Asia. *Asian Productivity Organization*, 1(1), 1-184.

¹¹² Sharma, A. (2020). Transaction returns/failures in DBT payments. <https://www.linkedin.com/pulse/transaction-returns-failures-dbt-payments-arun-sharma/>; Kale, S., Bhandari, L., and Nageswaran, V. A. (2021). *Direct Benefit Transfers: Status and challenges ahead*. Indicus Foundation. https://www.indicus.org/admin/pdf_doc/Direct-Benefit-Transfer-Status-and-Challenges-Ahead.pdf.

¹¹³ NPCI. (n.d.). *Product statistics – NACH Credit*. <https://www.npci.org.in/product/nach/product-statistics>

However, the reported magnitude of fiscal savings attributed to DBT remains contested. Reported reductions in expenditure or beneficiary counts are often interpreted as efficiency gains, but such estimates lack a clear counterfactual¹¹⁴ and may reflect both improved targeting and unintended exclusion of eligible beneficiaries.¹¹⁵ Stakeholders also highlighted the absence of standardised frameworks for distinguishing between de-duplication, reduced leakages, administrative efficiencies and notional savings estimates. Recent audit findings further suggest that weaknesses in beneficiary databases and verification systems continue to affect programme integrity. In 2025, the Comptroller and Auditor General (CAG) reported multiple instances of welfare payments being released without adequate verification, including transfers to ineligible or unverified beneficiaries across several schemes.¹¹⁶ These findings indicate that improvements in payment infrastructure do not automatically eliminate weaknesses in underlying administrative records.

Data quality remains a challenge. While Aadhaar incorporates biometric and demographic de-duplication mechanisms and the UIDAI periodically cancels duplicate records, maintaining accurate beneficiary databases requires continuous updating across multiple government systems.¹¹⁷ Limited integration between Aadhaar and civil registration databases has resulted in records linked to deceased individuals continuing to remain active.¹¹⁸ A Right to Information (RTI) response in 2025 indicated that only about 1.17 crore Aadhaar numbers had been deactivated against an estimated 16 crore deaths since Aadhaar's inception.¹¹⁹ In the absence of regular reconciliation with civil registration and death records, such inactive identities can persist within beneficiary databases, creating opportunities for fraud, inflating beneficiary lists and weakening the efficiency gains expected from accurate targeting and de-duplication.¹²⁰ Addressing these challenges requires moving beyond one-time identification towards continuous database updating, improving interoperability across administrative systems¹²¹ and enabling family-based reporting of deaths.¹²²

¹¹⁴ RUPE India. (2024, May). *Spurious claims of giant fiscal savings; grim realities*.

¹¹⁵ Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106 (10): 2895–2929. <https://www.aeaweb.org/articles?id=10.1257/aer.20141346>

¹¹⁶ Moneylife Digital Team. (2025, December 18). CAG says thousands of crores of rupees flowing into DBT accounts without checks: Report. *Moneylife*. <https://www.moneylife.in/article/cag-says-thousands-of-crores-of-rupees-flowing-into-dbt-accounts-without-checks-report/79156.html>

¹¹⁷ Upadhyay, A. (2025, July 16). Millions dead, Aadhaar still active: RTI finds only 1.15 crore cards deactivated. *India Today*. <https://www.indiatoday.in/india/story/millions-dead-aadhaar-still-active-rti-finds-only-115-crore-cards-deactivated-2756437-2025-07-16>

¹¹⁸ Times of India Desk. (2025, July). UIDAI move to deactivate Aadhaar of deceased sparks concerns over accuracy, process. *The Times of India*. <https://timesofindia.indiatimes.com/city/pune/uidai-move-to-deactivate-aadhaar-of-deceased-sparks-concerns-over-accuracy-process/articleshow/122866245.cms>

¹¹⁹ India Today. (2025, July 16). Millions “dead”, Aadhaar still active: RTI finds only 1.15 crore cards deactivated. <https://www.indiatoday.in/india/story/millions-dead-aadhaar-still-active-rti-finds-only-115-crore-cards-deactivated-2756437-2025-07-16>

¹²⁰ See Table 2.2 of Appendix 2 for examples of frauds.

¹²¹ Ministry of Electronics & IT. (2025, July 16). *UIDAI takes proactive measures to maintain continued accuracy & integrity of the Aadhaar database by deactivating Aadhaar numbers of deceased persons*. Press Information Bureau. https://uidai.gov.in/images/Press_Release-15.pdf

¹²² India Today. (2025, July 16). Millions “dead”, Aadhaar still active: RTI finds only 1.15 crore cards deactivated. <https://www.indiatoday.in/india/story/millions-dead-aadhaar-still-active-rti-finds-only-115-crore-cards-deactivated-2756437-2025-07-16>

Emerging evidence from scheme-level implementation complicates the efficiency narrative. Investigations into DBT-related fraud in Rajasthan revealed instances of duplicate or fictitious beneficiaries receiving payments across multiple schemes, including PM-KISAN, pensions and disaster relief programmes, highlighting gaps in cross-database verification.¹²³ Additionally, rising refill prices and affordability constraints have affected continued LPG usage among poorer households,¹²⁴ indicating that direct transfers alone may not fully address access barriers where underlying purchasing power remains limited. These findings suggest that improvements in administrative efficiency may not uniformly translate into effective or equitable welfare delivery on the ground.

3.5.2 Time and User-Side Efficiency

DBT can improve efficiency by reducing delays in fund disbursement and making payment processes more predictable through digitised and standardised systems, as seen in employment and pension schemes in Andhra Pradesh.¹²⁵ However, these gains are not uniform across schemes and contexts. Implementation experience indicates that administrative bottlenecks, system-level delays and compliance requirements can significantly affect timeliness. For instance, despite a digital transfer architecture, [NIKSHAY](#) payments for tuberculosis patients experienced a median delay of 101 days due to multiple layers of approval, overburdened frontline staff managing paper-based documentation, poor internet connectivity and technical issues in the NIKSHAY and PFMS portals.^{126,127} Thus, while DBT improves the speed and predictability of payments in principle, its realised efficiency depends on the reliability of implementation systems and the extent to which user-side frictions are minimised.

3.5.3 From Transfer Efficiency to Outcome Effectiveness

Improvements in transfer efficiency do not necessarily translate into effectiveness in achieving welfare outcomes. While DBT enhances the accuracy, speed and transparency of fund delivery, its impact ultimately depends on how transferred resources are used and whether they align with policy objectives. In India, most DBT schemes operate as unconditional cash transfers, which offer administrative simplicity and provide beneficiaries

¹²³ NH Digital. (2026, February 23). Multi-scheme DBT scam unearthed in Rajasthan: PM-Kisan, pension, disaster relief targeted. *National Herald*. <https://www.nationalheraldindia.com/national/multi-scheme-dbt-scam-unearthed-in-rajasthan-pm-kisan-pension-disaster-relief-targeted>

¹²⁴ Powell, L., Sati, A., & Tomar, V. K. (2023, September 12). *Limits to subsidising access to Liquefied Petroleum Gas in India*. Observer Research Foundation. <https://www.orfonline.org/english/expert-speak/limits-to-subsidising-access-to-liquefied-petroleum-gas-in-india>

¹²⁵ Muralidharan, K., Niehaus, P., and Sukhtankar, S. (2016). Building state capacity: Evidence from biometric smartcards in India. *American Economic Review*, 106 (10): 2895–2929. DOI: 10.1257/aer.20141346

¹²⁶ Nirgude, A. S., Kumar, A. M. V., Collins, T., Naik, P. R., Parmar, M., Tao, L., Akshaya, K. M., Raghuveer, P., Yatnatti, S. K., Nagendra, N., Nagaraja, S. B., Habeena, S., Mn, B., Rao, R., & Shastri, S. (2019). 'I am on treatment since 5 months but I have not received any money': Coverage, delays and implementation challenges of 'Direct Benefit Transfer' for tuberculosis patients – A mixed-methods study from South India. *Global Health Action*, 12(1), 1633725. <https://doi.org/10.1080/16549716.2019.1633725>

¹²⁷ Chauhan, V. (2026). *TB patients in UP struggle as aid gets delayed in Centre's scheme*. Times of India. <https://timesofindia.indiatimes.com/city/lucknow/tb-patients-in-up-struggle-as-aid-gets-delayed-in-centres-scheme/articleshow/126443135.cms>

with flexibility in spending.¹²⁸ However, the fungibility of cash implies that transfers may not always be directed towards intended outcomes such as improved nutrition, education or productive investment.

This highlights a fundamental trade-off: unconditional transfers are simpler to allocate but may weaken the link between public expenditure and targeted welfare outcomes, and conditional transfers, while more effective, may increase risks of exclusion and compliance burdens.¹²⁹ As a result, there is growing interest in hybrid instruments such as vouchers and digitally targeted transfers such as e-RUPI that seek to combine the flexibility of cash with greater alignment to policy objectives.¹³⁰

This also reflects the risk captured in Goodhart's law: when a measure becomes a target, it can cease to be a good measure. Indicators such as transaction completion rates, Aadhaar seeding, leakage reduction and fiscal savings are useful but may become misleading if treated as proxies for welfare success in themselves. A narrow focus on measurable efficiency can obscure less visible costs, including wrongful exclusion, unresolved payment failures, beneficiary time burdens, reduced discretion at the front line and weakened grievance redress. DBT evaluation should therefore balance administrative metrics with outcome-based and user-centric indicators.

3.6 Security, Privacy and Cybersecurity

In the context of DPI-enabled welfare systems, security extends beyond technical questions of cybersecurity and fraud prevention. Drawing on the security dimension of the evaluation framework, this section adopts a holistic conception of security encompassing privacy and data protection (including elements such as privacy by design and data storage), cybersecurity and resilience, fraud prevention, and governance and compliance. Stakeholder consultations highlighted that security is closely linked to the broader trustworthiness of the system, encompassing trust in authentication mechanisms, the accuracy and integrity of beneficiary databases, the reliability of grievance redress mechanisms and the governance arrangements through which personal data is collected, processed, shared and protected. Security was therefore viewed not only as a question of safeguarding systems against external threats but also as a way of ensuring transparency, accountability and resilience that can sustain citizen trust in welfare delivery institutions.

¹²⁸ Joy, J. (2018). A critical analysis of direct benefit transfer in India. *Indian Journal of Economics and Development*, 6(8), 1-7.

¹²⁹ Joy, J. (2018). A critical analysis of direct benefit transfer in India. *Indian Journal of Economics and Development*, 6(8), 1-7.

¹³⁰ Stakeholder insights.

3.6.1 Privacy and Data Protection

The DBT ecosystem incorporates several “privacy by design”¹³¹ features within the Aadhaar architecture to limit the exposure and misuse of personal data. A key safeguard is the minimal disclosure principle embedded in Aadhaar authentication, which typically provides a “yes/no” response without sharing underlying demographic or biometric information. Additional mechanisms such as virtual IDs (VIDs),¹³² tokenisation¹³³ and the Aadhaar Data Vault (ADV)¹³⁴ framework further reduce the risks associated with identity linkage. These measures enable the use of temporary or masked identifiers instead of Aadhaar numbers and restrict the storage of sensitive identity data within departmental systems.¹³⁵

Though the Aadhaar Act, 2016, and the DPDP Act, 2023, contain provisions for access, correction and withdrawal of consent, beneficiaries often have limited effective choice when access to welfare entitlements hinges on successful Aadhaar authentication.¹³⁶ As a result, the distinction between voluntary and mandatory use becomes blurred,¹³⁷ making it difficult for individuals to meaningfully control how their data is processed without potentially sacrificing benefits or access to essential services.¹³⁸

From an architectural perspective, DBT has a hybrid structure. Core identity data, including biometrics, is stored within the Central Identities Data Repository (CIDR) managed by UIDAI, which has stringent security measures; for instance, authentication transactions are encrypted and requesting entities are subject to regulatory controls on data usage, retention and purpose limitation.¹³⁹ Programme-level data such as beneficiary records, bank account details and transaction histories is distributed across ministries, state governments, banks and payment intermediaries, enabling administrative flexibility. Such entities are formally recognised as data fiduciaries under the DPDP Act, 2023, but the aggregation of such data

¹³¹ “Privacy by design” was conceptualised by Dr. Anne Cavoukian in 1990 as a mechanism of designing digital systems with privacy controls embedded into their architecture and system functionalities from the onset, rather than as an afterthought – an idea that has since been adopted in numerous data protection regimes. Read here: <https://documents1.worldbank.org/curated/en/546691543847931842/pdf/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.pdf>

¹³² VID is a 16-digit number that may be used by individuals instead of their 12-digit Aadhaar number and can be changed by the users at will; the Aadhaar UID can only be reconstructed by using the VID provided by the UIDAI.

¹³³ Tokenisation involves the generation of a UID token by UIDAI when a user successfully authenticates through their UID or VID, which is stored by the agency or provider in their customer records.

¹³⁴ Express News Service. (2025, December 2). Delhi government fast-tracks Aadhaar vault project to safeguard citizens’ identity data. *The New Indian Express*. <https://www.newindianexpress.com/cities/delhi/2025/Dec/02/delhi-government-fast-tracks-aadhaar-vault-project-to-safeguard-citizens-identity-data>

¹³⁵ Gelb, A., & Mukherjee, A. (2025). *Aadhaar as proof of identity: Could tokenization offer a solution?* Center for Global Development. <https://www.cgdev.org/blog/aadhaar-proof-identity-could-tokenization-offer-solution>

¹³⁶ An argument raised by Justice Chandrachud in his dissent against the validity of the Aadhaar Act in *Justice KS Puttaswamy (Retd) v. Union of India* (2018)

¹³⁷ Ramanathan, U. (2018). The political meaning of privacy and identity: An interview with Usha Ramanathan. *Sur: International Journal on Human Rights*, 15(27). <https://sur.conectas.org/en/the-political-meaning-of-privacy-and-identity-an-interview-with-usha-ramanathan/>

¹³⁸ Bhatia, G. (2018, August 24). Has the privacy judgement made a visible difference to our lives? *The Wire*. <https://thewire.in/law/has-the-privacy-judgement-made-visible-difference-to-our-lives>

¹³⁹ Supreme Court Observer. (n.d.). *Constitutionality of Aadhaar (Justice K.S. Puttaswamy v. Union of India): Judgment in plain English*. <https://www.scoobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/>

across systems can create profiling risks and increase exposure to breaches, particularly where security standards vary across institutions.¹⁴⁰

High-profile cases, including the public disclosure of personal data, illustrate how identity data once seeded across multiple platforms can be aggregated and exposed through relatively simple vulnerabilities.¹⁴¹ These patterns suggest that security risks in DBT arise less from centralised biometric compromise and more from decentralised data governance challenges, including uneven enforcement, gaps in vendor oversight and risks of data aggregation across interoperable systems.¹⁴²

3.6.2 Cybersecurity Risks and System Vulnerabilities

Cybersecurity governance in India's DBT ecosystem is inherently multi-layered and distributed across identity infrastructure, financial intermediaries and implementing agencies. At the identity layer, the UIDAI has adopted a "defence-in-depth" architecture for Aadhaar, including continuous monitoring, periodic audits, ISO-certified security practices, independent application testing and advisories from the National Critical Information Infrastructure Protection Centre (NCIIPC) to guard against unauthorised access and cyber threats. The government has also stated that no breach of the Aadhaar database has occurred,¹⁴³ reflecting a centralised technical hardening of core identity systems.

Despite this, cybersecurity risk in DBT frequently manifests at the peripheral and interoperable layers. The distributed nature of welfare databases creates a broad attack surface with uneven security. The Ministry of Home Affairs' Indian Cyber Crime Coordination Centre (I4C) documented instances of biometric data cloned from publicly accessible databases, such as fingerprints from land records, to conduct unauthorised AePS withdrawals in 2023.¹⁴⁴ Vulnerabilities, including unmasked fingerprints on publicly available documents, weak KYC processes, absence of liveness detection and inadequate real-time alerts, highlight risks at the system edge and across supply chains.¹⁴⁵

Cybersecurity responsibilities are distributed across multiple regulatory and institutional actors. Banks and financial intermediaries are governed by the RBI's Cybersecurity

¹⁴⁰ Internet Freedom Foundation. *Initial statement on the notification of the Digital Data Protection Rules, 2025*. <https://internetfreedom.in/iffs-initial-statement-on-the-notification-of-the-digital-data-protection-rules-2025/>

¹⁴¹ Agarwal, S. (2018, July 30). TRAI chief's personal details leaked after he challenges to prove how Aadhaar can be misused. *Uma Technology*. https://umatechnology.org/tra-chiefs-personal-details-leaked-after-he-challenges-to-prove-how-aadhaar-can-be-misused/#google_vignette

¹⁴² Union Government. (2021). *Report of the Comptroller and Auditor General of India on Functioning of Unique Identification Authority of India*. https://cag.gov.in/uploads/download_audit_report/2021/24%20of%202021_UIDAI-0624d8136a02d72.65885742.pdf; Comptroller and Auditor General of India. Report no. 24 of 2021 - Union Government (Ministry of Electronics and Information Technology), Performance Audit on Functioning of Unique Identification Authority of India. <https://cag.gov.in/en/audit-report/details/116042>

¹⁴³ Statement by Minister of State (MeitY) Jitin Prasada, Lok Sabha, 17 December 2025. https://sansad.in/getFile/loksabhaquestions/annex/186/AU2855_Ls0eOU.pdf?source=pgals

¹⁴⁴ See more examples of such frauds in Table 2.2 of Appendix 2.

¹⁴⁵ Das, M. (2023). Cybercriminals 'cloning' Aadhaar biometric data to commit fraud: MHA nodal agency to states. *The Print*. <https://theprint.in/india/governance/cybercriminals-cloning-aadhaar-biometric-data-to-commit-fraud-mha-nodal-agency-to-states/1415112/>

Framework,¹⁴⁶ while the NPCI¹⁴⁷ issues operational controls for payment systems. Government entities are required to report incidents to the Indian Computer Emergency Response Team (CERT-In) within six hours of detection under the CERT-In Directions of April 2022.¹⁴⁸ Under the DPDP Rules, 2025, data fiduciaries must notify the Board and affected data principals of personal data breaches without delay.¹⁴⁹ While these overlapping mechanisms enhance systemic visibility, they can also complicate coordination during multi-actor incidents.

In principle, a range of technical safeguards are embedded within the DBT ecosystem, but the heterogeneous implementation across jurisdictions and actors limits the effectiveness of these safeguards in practice. The absence of aggregate metrics on intrusion attempts, detection rates, coordinated response outcomes and publicly available information on the conduct of privacy impact assessments constrains independent evaluation of system-wide security and resilience.

An assessment of the security of the DBT ecosystem also raises a question about operational resilience. Because welfare payments are essential services, security risks are not limited to unauthorised access or data exposure; they also include the continuity of benefit delivery during authentication failures, cyber incidents, payment disruptions or fraud events. Assessing DBT's security therefore requires attention to detection and recovery timelines, institutional responsibility for containment and remediation and the extent to which beneficiaries are protected from bearing the costs of service failure.

3.6.3 Fraud Risks

Fraud remains a persistent concern in India's DBT ecosystem, reflecting both its scale and the multiplicity of actors involved.¹⁵⁰ While safeguards exist across the delivery chain, risks continue to emerge due to gaps in implementation and coordination.

At the enrolment stage, biometric de-duplication within the CIDR and the 2025 tightening of KYC norms, such as real-time document verification and cross-database checks, aim to prevent duplicate or ghost identities.¹⁵¹ At the transaction level, banks and payment system participants are required to undertake fraud monitoring, anomaly detection and reporting of

¹⁴⁶ It mandates board-approved security policies, security operations centres, vulnerability assessments and penetration testing, and timely reporting of cyber incidents to the RBI. Reserve Bank of India. (June 2016). *Cyber Security Framework in Banks*. Circular DBS.CO/CSITE/BC.11/33.01.001/2015-16. <https://www.rbi.org.in/commonman/english/scripts/Notification.aspx?Id=1721>

¹⁴⁷ Economic Times. (December 2023). *How NPCI is in action to curb Aadhaar-enabled Payment System (AePS) frauds*. <https://bfsi.economictimes.indiatimes.com/news/banking/how-npci-is-in-action-to-curb-aadhaar-enabled-payment-system-aeps-frauds/106274330>

¹⁴⁸ Majumdar, A. et al. (August 2023). Cyber security: India revamps rules on mandatory incident reporting & allied compliances. *The National Law Review*. <https://natlawreview.com/article/cyber-security-india-revamps-rules-mandatory-incident-reporting-allied-compliances>

¹⁴⁹ MeitY. (November 2025). *Digital Personal Data Protection Rules 2025, Rule 7*. THE GAZETTE OF INDIA: Extraordinary. <https://www.meit.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf>

¹⁵⁰ A list of frauds related to data leaks, security, falsification of identity and Aadhaar is provided in Table 2.2 of Appendix 2.

¹⁵¹ Rai, S. (2025, July 11). Aadhaar enrolment: New UIDAI norms, verification, fraud checks. *Business Standard*. https://www.business-standard.com/india-news/aadhaar-enrolment-new-uidai-norms-verification-fraud-checks-125071100821_1.html

suspicious transactions under RBI's fraud risk framework,¹⁵² while the UIDAI regulates authentication entities through security standards and audit requirements.

Recent interventions, including AI-based liveness detection systems and the Security and Trust in AI (SITAA) programme, have sought to enhance system resilience and address emerging threats such as biometric spoofing and deepfake-enabled fraud, particularly in high-volume schemes.^{153,154} Despite these layered safeguards, monitoring capacity remains uneven across the ecosystem, particularly at the last-mile interface involving BCs and local operators.

3.6.4 Cloud Infrastructure, Data Storage and Emerging Risks

An additional layer of complexity arises from the cloud infrastructure supporting DBT systems. Under the Government of India's GI Cloud (MeghRaj) framework,¹⁵⁵ public-sector data is hosted on empanelled cloud service providers, including both government-operated and private infrastructure, with localisation requirements. The sector-specific regulations impose tighter controls for sensitive identity data. UIDAI's Circular No. 14 of 2025¹⁵⁶ reinforces the ADV framework by mandating the tokenised storage of Aadhaar numbers and restricting the use of raw identifiers, while permitting cloud deployment only within controlled environments, such as on-premise systems or government community clouds (GCCs), subject to strict encryption and access controls. This reflects a shift towards a vault-based, privacy-preserving architecture.

However, the continued reliance on cloud-based architectures introduces long-term vulnerabilities linked to evolving technological threats. The current encryption standards may be susceptible to quantum computing advances, prompting early discussions within UIDAI on transitioning towards post-quantum cryptography (PQC) to future-proof identity systems.¹⁵⁷ However, such transitions remain complex and nascent.

¹⁵² RBI. *Master directions on fraud risk management in commercial banks (including regional rural banks) and All India Financial Institutions*, 2024-25. https://m.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12702

¹⁵³ Ministry of Electronics & IT. (2023, February 23). *UIDAI rolls out new security mechanism for robust fingerprint based Aadhaar authentication*. Press Information Bureau. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1902822>

¹⁵⁴ Unique Identification Authority of India. (n.d.). *UIDAI launches Scheme for Innovation and Technology*. https://uidai.gov.in/images/UIDAI_launches_Scheme_for_Innovation_and_Technology.pdf

¹⁵⁵ Nishith Desai Associates. (2018, April 5). *MeghRaj: India's Cloud Initiative*. https://nishithdesai.com/Content/document/pdf/Quotes/180405_Q_indrastra.com-MeghRaj_Indias_Cloud_Initiative.pdf

¹⁵⁶ Unique Identification Authority of India. (2025). *Circular No. 14 of 2025*. https://uidai.gov.in/images/Circular-No.14_of-2025.pdf. For more such cases, see Table 2.2 of Appendix 2.

¹⁵⁷ Stakeholder insights.

Box 3: Post-Quantum Cryptography and Risks to the DBT system

Post-Quantum Cryptography and Risks to the DBT system

Aadhaar-enabled DBT systems rely on encryption that secures identity and transaction data by making the data computationally unfeasible to “unlock” using current computers. However, advances in quantum computing could undermine this foundation by enabling the decryption of widely used public-key systems.¹⁵⁸ While not an immediate threat, the key risk lies in a “harvest now, decrypt later” dynamic. When cryptographically relevant quantum computers become available, this archived data could be decrypted retrospectively.¹⁵⁹

India has begun exploring quantum resilience, including considering next-generation encryption under UIDAI’s Aadhaar Vision 2032 framework. However, the integration of PQC remains at a nascent stage without a clear deployment pathway.¹⁶⁰ For India, the scale of the challenge is immense, involving the migration of the cryptographic foundation of a digital identity system that serves over 1.4 billion residents and supports more than 2 billion authentication transactions every month.¹⁶¹ Moreover, PQC algorithms impose larger key sizes and computational overhead. In a system processing millions of daily authentication requests across rural low-bandwidth environments, last-mile latency implications of Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) adoption are likely to pose a challenge.¹⁶²

Given the long-lived sensitivity of identity data, delaying transition to quantum-resistant cryptography risks retroactive compromise, making early adoption of cryptographic agility and a coordinated migration roadmap crucial, especially as global standard-setting efforts are already advancing PQC adoption timelines.¹⁶³

3.6.5 Grievance Mechanisms for Security Breaches

Addressing security breaches and fraudulent transactions within the DBT ecosystem presents distinct challenges compared to general service-related grievances. Redress mechanisms remain fragmented across institutions, and beneficiaries often face difficulties in identifying the appropriate authority for redress, particularly when failures span multiple layers of the

¹⁵⁸ Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). IEEE. doi: 10.1109/SFCS.1994.365700.

¹⁵⁹ Microchip Technology Inc. (2025). *Post-quantum cryptography and “harvest now, decrypt later” threats*. <https://www.microchip.com/en-us/about/media-center/blog/2025/post-quantum-cryptography-harvest-now-decrypt-later-threats>

¹⁶⁰ Unique Identification Authority of India. (2025). *Aadhaar vision 2032: Future-proofing digital identity*. Government of India. https://uidai.gov.in/images/UIDAI_initiates_Technological_and_Strategic_Review_to_shape_the_future_of_Digital_ID.pdf

¹⁶¹ Unique Identification Authority of India. (n.d). *Aadhaar Dashboard*. https://uidai.gov.in/aadhaar_dashboard/index.php

¹⁶² Joe, S. (2025, November). Post-quantum cryptography: India’s migration strategy. *The Medium*. <https://medium.com/@sankalpi17/post-quantum-cryptography-indias-migration-strategy-5d406793604f>

¹⁶³ Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (November 2024). *Transition to post-quantum cryptography standards*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8547.ipd>; Global Risk Institute. (2025, September 3). *Quantum threat timeline report 2024*. <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>

system. Delays in resolution, institutional coordination and challenges in establishing liability further complicate the process. This is especially pronounced in cases involving Aadhaar-enabled payment systems, where disputes may involve banks, BC agents and authentication infrastructure providers.¹⁶⁴

UIDAI grievance redress mechanisms,¹⁶⁵ scheme-specific portals and government grievance platforms like the Central Public Grievance Redressal and Monitoring Systems (CPGRAMS),¹⁶⁶ banking ombudsman channels under RBI frameworks¹⁶⁷ and administrative complaint systems are available for beneficiaries to file complaints. The DPDP Rules, 2025, also introduced breach notification obligations and a Data Protection Board for adjudication.¹⁶⁸ However, the availability of multiple redress channels does not by itself ensure effective remedy when responsibility is distributed across several actors.

A resilient DBT system requires a single, accessible route for reporting security breaches, fraudulent transactions and payment failures, supported by clear inter-agency responsibility for investigation, end-to-end case tracking, defined resolution timelines and continuity protections where an entitlement is at risk. Before seeking redress, beneficiaries should not be required to determine whether a failure originated with Aadhaar, a scheme database, PFMS, a bank, NPCI, a BC or an authentication provider.

3.7 Recommendations

The DBT experience demonstrates both the transformative potential and the evolving challenges of DPI-enabled welfare delivery. While the system has significantly improved the scale, transparency and efficiency of public transfers, it also highlights persistent tensions between inclusion, efficiency and security. Exclusion risks continue to arise from beneficiary identification and last-mile access challenges; efficiency gains remain dependent on data quality and implementation capacity; and growing reliance on interconnected digital systems has elevated the importance of security, accountability and public trust. Building on these findings, we propose some recommendations to strengthen DBT as a citizen-centric, outcome-oriented and resilient welfare delivery architecture (Table 4).

¹⁶⁴ Drèze, J. & Paikra, V. (2021). Loopholes in Aadhaar-enabled payment system putting poor people at risk. *The Indian Express*. <https://indianexpress.com/article/opinion/columns/aadhaar-enabled-payment-system-7552163/>

¹⁶⁵ UIDAI. *Grievance redressal mechanism*. <https://uidai.gov.in/en/contact-support/grievance-redressal.html>

¹⁶⁶ Department Of Administrative Reforms & Public Grievances Central Public Grievance Redressal and Monitoring System (CPGRAMS). <https://dargp.gov.in/en/public-grievances>

¹⁶⁷ Reserve Bank of India – Integrated Ombudsman Scheme, 2021. <https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?id=3407>

¹⁶⁸ Press Information Bureau. (2025, November 17). *DPDP Rules, 2025. A citizen-centric framework for privacy protection and responsible data use*. <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf>

Table 4: Strategic Priorities for the Next Phase of DBT

Priority Area	Strategic Focus	Desired Outcome
Inclusion & Last-Mile Delivery	Reduce exclusion by improving authentication, portability, assisted-service delivery, and beneficiary visibility across the welfare ecosystem	More accessible, inclusive and citizen-centric welfare delivery
Outcome-Oriented Service Delivery	Move beyond transfer efficiency towards stronger data quality, proactive service delivery, interoperability, and outcome monitoring	Improved welfare outcomes and reduced administrative burden
Security, Accountability & Public Trust	Strengthen ecosystem-wide security, privacy safeguards, accountability frameworks, beneficiary rights and integrated fraud monitoring	Greater trust, transparency and resilience of welfare systems
Future-Ready & Resilient Infrastructure	Build adaptive infrastructure through interoperability, edge DPI, cryptographic agility and continuous innovation	Long-term sustainability and preparedness for emerging risks

Strengthen Citizen-Centric Inclusion and Last-Mile Delivery

Despite progress in expanding financial inclusion and digital access, exclusion risks continue to arise from authentication failures, database inaccuracies, portability constraints and administrative burdens placed on beneficiaries. Future reforms should focus not only on expanding scale but also on improving the lived experience of beneficiaries.

- Institutionalise alternative authentication and exception-handling mechanisms to ensure continuity of service when digital verification fails.
- Shift from beneficiary-led correction processes to proactive updating of records through periodic audits and inter-agency data validation.
- Strengthen portability of welfare entitlements, particularly for migrants and mobile populations.
- Expand investment in last-mile support systems, including BCs, Bank Sakhis, CSCs and other assisted-service models.
- Develop an integrated citizen-facing DBT dashboard providing end-to-end visibility into the transfer lifecycle, including eligibility determination, benefit status, authentication outcomes, payment flows and grievance resolution across schemes.

Move from Transfer Efficiency to Outcome-Oriented Service Delivery

Efficient fund transfer must be regarded as a means and not an end in itself. The next phase of DBT must broaden its metrics of success beyond leakage reduction and fiscal savings to encompass improvements in welfare outcomes, reduction in administrative burden for citizens and improvements in the quality of entitlement delivery.

- Strengthen transparency and methodological rigour in estimating efficiency gains, distinguishing between de-duplication effects, exclusion and genuine efficiency improvements.
- Improve beneficiary databases through continuous updating, de-duplication and verification, treating data quality as ongoing infrastructure maintenance rather than a one-time exercise.
- Strengthen interoperability across central and state welfare systems to reduce duplication and enable a whole-of-government approach to service delivery.
- Advance proactive service delivery models, including automated eligibility determination and beneficiary identification where appropriate.
- Establish systematic monitoring of exclusion, service quality and beneficiary outcomes alongside existing efficiency metrics.
- Reduce documentation and verification burdens through trusted digital credentials and informed consent-based data sharing under a robust privacy framework.

Strengthen Security, Accountability and Public Trust

As DBT systems become increasingly interconnected, security must be viewed within the broader context of system trustworthiness rather than just for protection against cyberattacks. Trust depends on the security of technical infrastructure, the integrity of beneficiary databases, the clarity of institutional accountability and the ability of citizens to understand, challenge and seek redress for decisions affecting their welfare benefits.

- Adopt an ecosystem-wide security approach that extends beyond Aadhaar to include banks, payment intermediaries, service providers and local implementation infrastructure.
- Strengthen the implementation of existing privacy-by-design principles by ensuring consistent adoption of data minimisation, purpose limitation, tokenisation, secure API governance and periodic privacy impact assessments across all participating entities.
- Develop clear accountability frameworks defining institutional responsibilities for security incidents, authentication failures, fraud and service disruptions.
- Strengthen beneficiary rights through improved transparency, auditability of welfare decisions and accessible mechanisms for correction and appeal.
- Establish integrated fraud-monitoring and incident-response systems capable of addressing emerging risks, including AI-enabled fraud and identity misuse.

Build Future-Ready and Resilient Digital Infrastructure

As DBT evolves towards more integrated and automated welfare delivery, technical architecture must be designed not only to meet the current scale but also for long-term

resilience, adaptability and security. Future infrastructure investments must ensure that welfare systems remain secure, usable and responsive to emerging risks while continuing to support innovation and scale.

- Invest in “edge DPI” and user-facing infrastructure that improves usability, explainability and citizen control over digital interactions with welfare systems.
- Strengthen interoperability standards while maintaining robust safeguards against excessive data aggregation, cross-programme profiling and surveillance risks.
- Build cryptographic agility into the DBT ecosystem and develop a phased roadmap for transition to post-quantum cryptography standards.
- Expand structured collaboration between government, academia and technical experts to support continuous innovation, independent security evaluation and rigorous assessment of DPI systems.

The next phase of DBT should move beyond a narrow focus on digitalising transfers towards building a citizen-centric, outcome-oriented, trustworthy and resilient welfare architecture. Policymakers must treat inclusion, accessibility, efficiency and security not as competing objectives but as mutually reinforcing pillars of effective public service delivery. Thus, the success of DPI-enabled welfare systems will require continuous investment in institutional capacity, data quality, accountability mechanisms and resilient digital infrastructure.

3.8 Comparative Analysis: DPI-Enabled Welfare Delivery in India and Australia

The collaboration between researchers in India and Australia to examine the role of DPI and public service delivery for this project provided an opportunity to reflect on how different institutional contexts shape the design and governance of digitally enabled welfare systems and generated valuable insights for both countries.

While both India and Australia have leveraged digital technologies to modernise welfare delivery, their systems have evolved in response to their different institutional contexts and policy priorities. The design of their digital ecosystems reflects distinct approaches to achieving inclusion, efficiency and security. Table 5 provides a comparison of the two systems across key dimensions of DPI, including the principal design choices and trade-offs that shape their respective welfare delivery models.

Table 5: Three-Pillar Comparison of India's and Australia's DPI Architectures for Welfare Delivery

Dimension	India (Aadhaar-Linked DBT)	Australia (myGov-Linked DBT)
DPI Technical Architecture		
Institutional Starting Point	DPI evolved primarily to strengthen state capacity by addressing fragmented beneficiary databases, subsidy leakages and financial exclusion.	Digital welfare evolved within mature administrative institutions, focusing on service integration, coordination and user experience.
Architectural Approach	Hybrid architecture centred on common digital rails (identity, payments and scheme databases) that enable interoperability across multiple implementing agencies.	Federated architecture where identity, payments and welfare administration remain institutionally distinct but interoperable through coordinated digital services.
Governance Model	Multi-agency governance distributes implementation responsibilities across central ministries, states, banks and ecosystem participants, allowing flexibility but increasing coordination complexity.	Service delivery is concentrated within a lead agency, enabling more uniform implementation, clearer accountability and streamlined coordination.
Design Philosophy	Common digital infrastructure is designed to create reusable public infrastructure that can be leveraged across multiple welfare schemes.	Digital infrastructure primarily strengthens integration of existing public services rather than serving as a common foundational layer across government.
Pillar 1: Accessibility & Inclusivity		
Participation Model	Welfare access is largely Aadhaar-linked, with digital identity effectively becoming the gateway for accessing most DBT schemes. The model prioritises broad population coverage through a common identity infrastructure.	Welfare services are universally available through Services Australia. Digital Identity (myID) remains voluntary for most services and is used selectively for higher-assurance transactions, prioritising flexibility over uniform identity integration.
Authentication Model	Multiple authentication modes (biometrics, OTP, face authentication and offline verification) support diverse user contexts, but biometric dependence can create exclusion risks in cases of fingerprint or iris mismatch.	Multi-factor authentication combines device-based credentials, passkeys, facial scan and document verification, without in-person attendance
Offline and Assisted Access	Assisted-digital delivery through BCs, CSCs, IPPB and post offices extends welfare access where digital capability or banking infrastructure is limited.	Permanent service centres, mobile service units, multilingual telephone support and community outreach provide institutional assistance for users facing digital or accessibility barriers.

Dimension	India (Aadhaar-Linked DBT)	Australia (myGov-Linked DBT)
Grievance and User Support	Multiple grievance channels exist across schemes and institutions. However, beneficiaries often need to identify the source of failure across different entities before seeking redress.	User support is delivered through a more integrated administrative framework with clearer escalation pathways and access to independent review mechanisms.
Pillar 2: Efficiency		
Source of Efficiency Gains	Removing layers of intermediaries, minimising leakages from duplicate and phantom beneficiaries and enabling direct transfers.	Simplifying service delivery, reducing administrative burden and improving user experience.
Automation Model	Automation standardises beneficiary verification, fund routing and payment processing across schemes, reducing manual processing at scale.	Automation streamlines routine claims processing, allowing over 80% of new claims to be lodged through digital self-service while reserving human intervention for complex cases. ¹⁶⁹
Scale and System Capacity	Designed to support population-scale welfare delivery, with the DBT ecosystem serving 176 crore cumulative beneficiaries across 320+ schemes.	Integrated digital administration supports efficient delivery of around 200 payment types administered by a single agency, with more than 70,000 claims processed per day during the COVID-19 pandemic. ^{170,171}
Digital Integration and Interoperability	Aadhaar, PFMS and NPCI payment rails integrate identity, beneficiary verification, fund authorisation and payments, enabling seamless consent-based information and fund flows across schemes, ministries, banks and implementing agencies.	myGov Tell Us Once, Single Touch Payroll, NPP/PayID and the Consumer Data Right connect government agencies, employers and the banking system, enabling once-only reporting, real-time payments, automated eligibility assessment and consent-based data sharing. ^{172,173, 174,175}
Pillar 3: Security		

¹⁶⁹ Services Australia. (2026, July 23). *Centrelink*. Government of Australia. <https://www.servicesaustralia.gov.au/centrelink>

¹⁷⁰ Shorten, B. (2023, December). *Hazlehurst appointed CEO of Services Australia* [Media Release]. Minister for Government Services.

¹⁷¹ Services Australia. (2020). *Annual report 2019–20*. Government of Australia. <https://www.servicesaustralia.gov.au/sites/default/files/annual-report-2019-20v2.pdf>

¹⁷² World Bank. (2021). *Fast payment systems: Australia's New Payments Platform (NPP) case study*. https://fastpayments.worldbank.org/sites/default/files/2021-10/World_Bank_FPS_Australia_NPP_Case_Study.pdf

¹⁷³ Australian Taxation Office. (2019). *Single Touch Payroll (STP)*. Government of Australia. <https://www.ato.gov.au/businesses-and-organisations/hiring-and-paying-your-workers/single-touch-payroll>

¹⁷⁴ NPP Australia Ltd. (2020). *New payments platform – Submission to Senate Select Committee*. Parliament of Australia. <https://www.aph.gov.au/DocumentStore.ashx?id=c4788f5a-60c7-479a-8cc4-303ef0f0dadf>

¹⁷⁵ Australian Payments Plus. (2025). *NPP / Australia's Payment Future*. <https://www.auspayplus.com.au/solutions/npp>

Dimension	India (Aadhaar-Linked DBT)	Australia (myGov-Linked DBT)
Legal and Governance Framework	Aadhaar Act 2016, DPDP Act 2023; distributed governance (DBT Mission, UIDAI, state governments, NPCI, RBI) that requires seamless coordination	Layered statute base, including the Social Security Act 1991, Social Security (Administration) Act 1999, Digital Identity Act 2024, Privacy Act 1988, and CDR provisions, with federated multi-agency oversight. ¹⁷⁶
Identity and Data Architecture	Centralised biometric database storing enrolment data; welfare and transaction data is distributed.	Federated, privacy-by-design model where credentials are held on the user device and verified against distributed databases.
Privacy and Consent	Consent-based sharing exists; privacy-by-design is embedded through data minimisation, tokenisation, virtual IDs and purpose-limited authentication; implementation remains uneven across the ecosystem.	No central biometric store; multi-factor authentication (myID, passkeys, SMS and email), granular consent through CDR and independent privacy oversight underpin data handling. ^{177,178,179}
Oversight and Key Risks	Oversight is distributed across multiple institutions; risks at peripheral layers, including large-scale data breaches, numerous instances of fraud and biometric exclusion errors.	OAIC and ANAO provide independent oversight; trust damaged by the Robodebt automated-decision failure, COVID-19 surge capacity limits and vendor and surveillance controversies. ^{180,181}

¹⁷⁶ Parliament of Australia. (2024). *Digital Identity Act 2024*. No. 49, Royal Assent.

¹⁷⁷ The Mandarin. (2025). *Sticky notes: David Hazlehurst, Services Australia CEO*. <https://www.themandarin.com.au/287706-sticky-notes-david-hazlehurst-services-australia-ceo/>

¹⁷⁸ myGov. (n.d.). *Sign in to myGov*. Australian Government. <https://my.gov.au/en/about/help/mygov-website/sign-in-to-mygov>

¹⁷⁹ Locke, H. (2023). *Privacy + cyber year in review and what to expect in 2024*. <https://hamiltonlocke.com.au/privacy-cyber-year-in-review-and-what-to-expect-in-2024/>

¹⁸⁰ Royal Commission into the Robodebt Scheme. (2023). *Report*. Commonwealth of Australia.

¹⁸¹ Etax.com.au. (2020). *How to apply for Jobseeker payments at myGov and Centrelink*. <https://www.etax.com.au/apply-for-jobseeker-payments/>

The comparison underscores that there is no single model for DPI-enabled welfare delivery. India's approach emphasises scalable and interoperable digital infrastructure to support welfare delivery across a large and diverse beneficiary base, whereas Australia's approach focuses on integrating public administration and strengthening institutional accountability to improve service delivery. These contrasting approaches illustrate that effective DPI design is shaped not only by technological capabilities but also by the institutional context, governance arrangements and policy objectives within which it operates.

3.9 Conclusion

The chapter demonstrates that India's DBT programme represents one of the most significant applications of DPI for public service delivery at population scale. Built on the JAM trinity and supported by interoperable payment and public financial management systems, DBT has transformed welfare administration by improving the speed, transparency and monitoring of benefit transfers while expanding financial inclusion and reducing leakages. The comparison with Australia further illustrates that there is no single pathway for digital welfare delivery; rather, different institutional arrangements can achieve similar public service objectives depending on administrative capacity, governance structures and welfare priorities.

The analysis also highlights that the performance of DBT cannot be evaluated solely through administrative efficiency or fiscal savings. As the system has evolved, new policy and implementation challenges have emerged relating to beneficiary identification, authentication failures, last-mile delivery, grievance redressal, institutional coordination and data governance. The case studies underscore that inclusion, efficiency and security are not competing objectives but mutually reinforcing dimensions that must be balanced throughout the design, implementation and evolution of digital welfare systems.

The assessment also suggests that these trade-offs should not be viewed as shortcomings of DPI-enabled welfare delivery but as inherent features of a large-scale and continuously evolving public infrastructure. Strengthening such systems requires sustained institutional adaptation, technological innovation, implementation learning and stakeholder engagement. As digital technologies and citizen expectations continue to evolve, governance frameworks must remain responsive to emerging risks while ensuring that welfare systems remain inclusive, accountable and trusted.

The continued evolution of DBT, including initiatives such as digital registries and more proactive models of welfare delivery, presents significant opportunities to further strengthen public service delivery. However, realising this potential will depend not only on technological innovation but also on enhancing institutional coordination, improving citizen experience and building public trust through transparent, secure and accountable implementation.

4. Case Study: Ayushman Bharat Digital Mission

4.1 Introduction

Digitalisation in healthcare emerged from the need to address longstanding challenges of fragmented records, inefficient service delivery, duplicated services, weak disease surveillance and limited availability of real-time health data. In many low- and middle-income countries (LMICs), early digital health initiatives, including India's Health Management Information System,¹⁸² Rwanda's RapidSMS¹⁸³ platform and Bangladesh's District Health Information Software 2 (DHIS2) system,¹⁸⁴ have strengthened community-level data collection, supervision and maternal and child health monitoring. These initiatives helped transform fragmented and paper-based reporting into more integrated digital workflows, significantly strengthening health systems by streamlining data flows, improving care continuity, enhancing resource planning and supporting evidence-based policymaking.¹⁸⁵

While these initiatives improved reporting and access to health data, most of them were vertical and program-specific, focusing on maternal health, tuberculosis or HIV, among others. Consequently, health data remained fragmented and siloed across different providers and departments, hindering the management of chronic diseases, delaying early detection and limiting integrated and continuous care. The absence of interoperability resulted in duplication of efforts by health workers and reliance on their memory or paper-based transfers for critical patient history. Public health campaigns like immunisation drives and tuberculosis screenings often depended on manual or semi-digital tracking, resulting in duplication, exclusion errors and delays. These challenges stemmed not from technological limitations but from the lack of foundational digital infrastructure capable of unifying services.

Digital Public Infrastructure for Health (DPI-H) is a novel and evolving paradigm that emerged to address some of these challenges and has the potential to transform health systems across countries. It refers to a country's digital infrastructure that enables the creation of inclusive, scalable and user-driven applications through open, interoperable and reusable digital building blocks such as health IDs, shared health registries and open health networks.¹⁸⁶ Table 6 highlights key differences between traditional digitalisation efforts and the DPI-H approach.

¹⁸² Ministry of Health and Family Welfare. (n.d.). *Health Management Information System (HMIS)*. Government of India. <https://hmis.mohfw.gov.in/#/>

¹⁸³ Organisation pour le Développement de l'E-Santé dans les pays du Sud (ODESS). (2026). *RapidSMS Rwanda*. <https://www.odess.io/en/initiative/rapidsms-rwanda/>

¹⁸⁴ Hoque, M. R., Hasan, M. R., Chowdhury, E. K., Kabir, M. H., & Rahman, M. S. (2020). Strengthening District Health Information System (DHIS2) data quality and use: Bangladesh experience. *BMC Health Services Research*, 20(1), Article 545. <https://doi.org/10.1186/s12913-020-05322-2>

¹⁸⁵ Krishnan, A., Nongkynrih, B., Yadav, K., Singh, S., Gupta, V., & Kumar, A. (2010). Evaluation of computerized health management information system for primary health care in rural India. *BMC Health Services Research*, 10, Article 310. <https://doi.org/10.1186/1472-6963-10-310>

¹⁸⁶ Das, B., Waweru, W., & Kedia, M. (2025, November 5). *The DPI approach to building accessible and resilient health systems* (T20 South Africa Policy Brief, Task Force 2: Digital Transformation). T20 South Africa. https://t20southafrica.org/wp-content/uploads/2025/11/T20_TF2_SB2_PB2_DPIApproach.pdf

Table 6: Traditional Digitalisation vs. DPI-H

Aspect	Traditional Digitalisation	DPI-H
Architecture	Program-specific silos (e.g., HIV, reproductive and child health)	Interoperable systems with open APIs
Patient Records	Fragmented, no longitudinal history	Continuous, unified health records across facilities
Health ID	Multiple IDs or none at all	Single digital health ID (e.g., ABHA) across systems
Access to Services	Platform-centric	Service discoverability through decentralised networks across platforms
Health Campaigns	Fragmented beneficiary databases, repeated enumeration and duplicate targeting	Single source of truth, de-duplicated targeting using reusable registries
Public-Private Integration	Weak linkages	Seamless data exchange and consent-enabled access

Source: Authors' compilation from multiple websites

Unlike traditional digitalisation efforts that focused on individual programmes or institutions, DPI-H seeks to create a common digital foundation for the entire health ecosystem. By linking health data to individuals rather than facilities or software vendors, as in the case of legacy models, DPI-H enables a transition from institution-centric to citizen-centric service delivery. This reduces friction, empowers patients and unlocks the potential for personalised, proactive and portable care across both public and private sectors.

Ayushman Bharat Digital Mission: India's DPI-H Approach

The National Digital Health Mission, India's flagship DPI initiative in the health sector, was launched through a pilot across six union territories in August 2020,¹⁸⁷ followed by a national rollout as the Ayushman Bharat Digital Mission (ABDM) in September 2021.¹⁸⁸ The vision of the ABDM, as laid down in its strategy documents, is to establish an open and interoperable digital health ecosystem through a set of core building blocks and common standards for supporting universal coverage of healthcare in an efficient, inclusive and secure manner.^{189,190} It also seeks to reorient healthcare delivery in India from reactive to preventive care and from a provider-driven to a citizen-centric model by empowering patients with access and control over their health data while facilitating seamless discovery and interoperability of health services.¹⁹¹

¹⁸⁷ Press Information Bureau. (2022, April 7). *National Digital Health Mission completes successful pilot launch in six union territories*. Government of India. <https://www.pib.gov.in/PressReleaseFramePage.aspx?PRID=1813660>

¹⁸⁸ Press Information Bureau. (2022, April 7). *National Digital Health Mission completes successful pilot launch in six union territories*. Government of India. <https://www.pib.gov.in/PressReleaseFramePage.aspx?PRID=1813660>

¹⁸⁹ Ayushman Bharat Digital Mission. (n.d.). *ABDM building blocks*. Government of India. https://abdm.gov.in:8081/uploads/ABDM_Building_Blocks_v8_3_External_Version_eabb5c0f3_4_a96f40c645.pdf

¹⁹⁰ National Health Authority. (2020). *NDHM strategy overview*. Government of India. https://nha.gov.in/assets/uploads/NDHM_Strategy_Overview.pdf

¹⁹¹ Ayushman Bharat Digital Mission. (n.d.). *Accelerating digitisation in healthcare delivery*. Government of India. https://abdm.gov.in/strapi/cms/uploads/Accelerating_Digitisation_in_Healthcare_Delivery_v3_fad6fe700f.pdf

The mission's blueprint proposes a unified set of standards in areas like consent management, technical and semantic interoperability, and privacy and security. These standards aim to address the challenges arising from the use of diverse file types, data formats, and technologies and platforms, which hinder the smooth exchange of health information within a complex and diverse healthcare ecosystem.¹⁹² The technological building blocks comprise a unique health identifier and a set of registries and gateways that seek to address multifaceted challenges (Table 7).

Table 7: ABDM Components and Their Value Propositions

Component	Description	Challenges Addressed	DPI Value Proposition
Ayushman Bharat Health Account (ABHA) and ABHA Address	A 14-digit number with an optional user-friendly alphanumeric ABHA address (e.g., name@abdm).	Multiple identities hindering unique identification and patient tracking; Fragmented records limiting comprehensive viewing and sharing of medical history; Longer wait times	• Simplifies identification and verification of patients • Enables creation and consent-based sharing of longitudinal health records • Improves continuity of care and streamlining of OPD registrations
Registries: Healthcare Professionals Registry (HPR) and Healthcare Facility Registry (HFR)	HPR is a repository of verified practising healthcare professionals, including doctors and nurses, identified by a unique health professional ID. HFR and the associated Health Facility ID provide a directory of public and private health facilities across the country, including hospitals, clinics, labs and pharmacies.	Lack of trusted registry of healthcare practitioners and facilities; Fragmented registration; Limited online presence and discoverability	• Improves trust and discoverability of authentic healthcare providers • Facilitates onboarding on various healthcare applications and online service delivery • Eases access to processes such as licensing and empanelment through consent-based sharing of standardised records • Provides a window for regulatory authorities to track professionals and facilities
Health Information Exchange-Consent Manager (HIE-CM)	A core digital gateway under ABDM that facilitates secure, consent-based exchange of health records within the ecosystem.	Siloed health records across institutions; Patients lack control over health data access and sharing	• Facilitates creation of longitudinal medical history, thereby enabling continuity of care and reducing duplicate testing • Enhances privacy and security through decentralised data exchange
Unified Healthcare	An open, interoperable network	A closed platform-centric model limiting demand-	• Facilitates supply- and demand-side players to be

¹⁹² Ministry of Health and Family Welfare. (2019). *Final report on National Digital Health Blueprint (NDHB)*. Government of India. https://mohfw.gov.in/sites/default/files/Final%20NDHB%20report_0.pdf

Interface (UHI)	for various digital health services such as teleconsultations, appointment booking and service discovery. ¹⁹³	supply ecosystems, constraining choice and control of participants over applications and pricing and creating fragmented markets for digital health services ¹⁹⁴	connected through apps of their choice • Ensures better accessibility and wider coverage of services ¹⁹⁵
National Health Claims Exchange (NHCE)	An open, standardised protocol for the seamless exchange of health claims data among relevant stakeholders – payors, providers, beneficiaries and regulatory bodies.	Manual and non-standardised claims adjudication processes reducing transparency, increasing processing costs, delaying payments and being complex and time-consuming for patients/policyholders ¹⁹⁶	• Provides standard formats and a single interface for data exchange among stakeholders, and streamlines health insurance claims processing • Enables better data quality and analytics and improves patient experience ¹⁹⁷

Source: Authors' own, from ABDM official documents

The ecosystem that drives the adoption and use of these components consists of entities across various stakeholder categories in the public, private and not-for-profit sectors (Figure 7). These stakeholders set the strategic direction and guidelines as well as the development, testing and implementation of use cases. Stakeholder alignment and coordination across this complex ecosystem have been managed through various governance institutions and processes, which are further explained in section 4.3.

¹⁹³ Ayushman Bharat Digital Mission. (n.d.). *Unified Health Interface (UHI)*. Government of India. <https://abdm.gov.in/uhi>

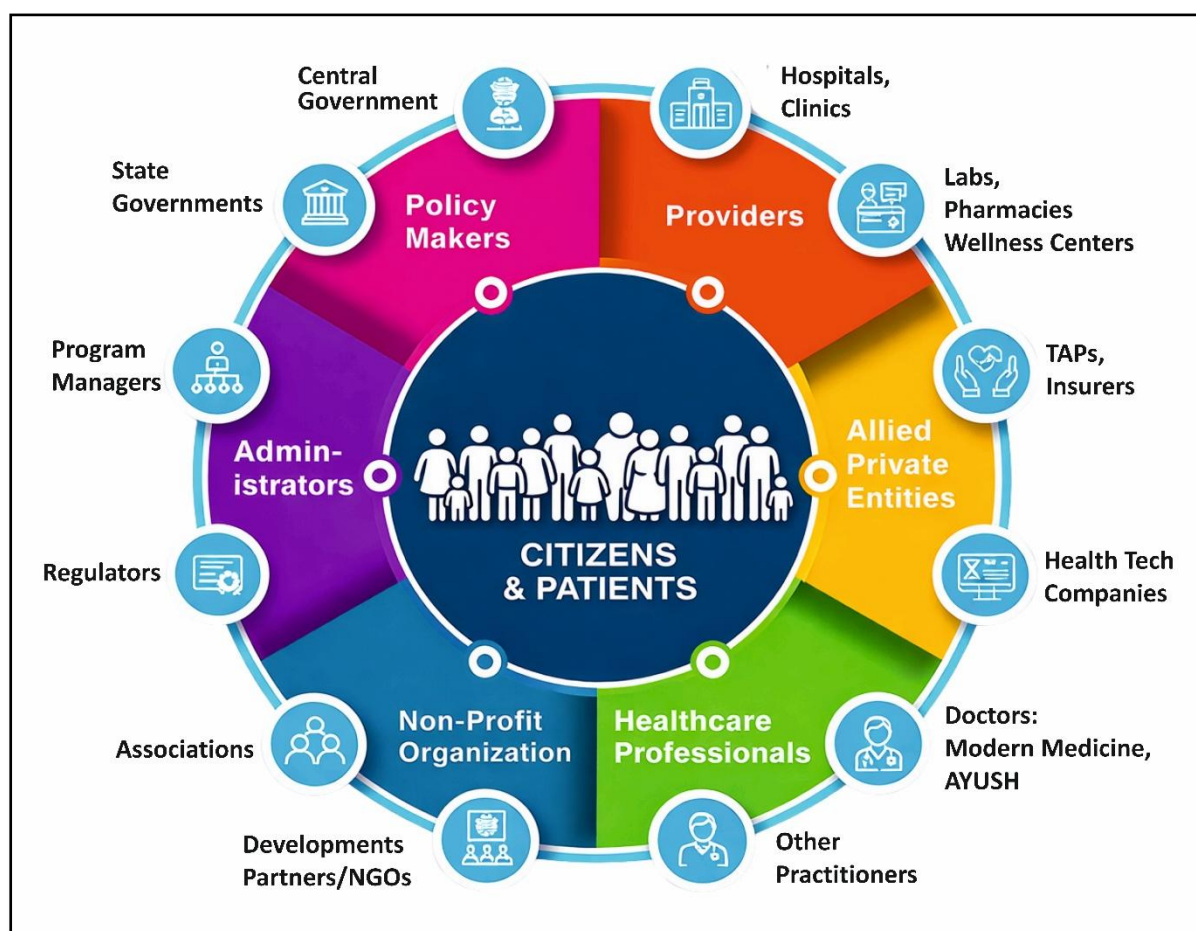
¹⁹⁴ Ayushman Bharat Digital Mission. (n.d.). *Synopsis: Operationalising Unified Health Interface (UHI) in India*. Government of India. https://abdm.gov.in:8081/uploads/Synopsis_Operationalising_Unified_Health_Interface_UHI_in_India_308cd449fb.pdf

¹⁹⁵ T20 South Africa. (2025). *The DPI approach to building accessible and resilient health systems*. https://t20southafrica.org/wp-content/uploads/2025/11/T20_TF2_SB2_PB2_DPIApproach.pdf

¹⁹⁶ National Health Authority. (n.d.). *Health Claims Exchange (HCE) Sandbox*. Government of India. <https://hcxsbx.abdm.gov.in/#/>

¹⁹⁷ Ayushman Bharat Digital Mission. (n.d.). *National Health Claims Exchange (NHCE) brochure*. Government of India. https://abdm.gov.in:8081/uploads/NHCE_Brochure_ffdb63d9bc.pdf

Figure 7: The ABDM Ecosystem



Source: National Health Authority (NHA)

Growth of the ABDM Building Blocks and Ecosystem

Since the launch of the mission, there has been considerable progress in uptake. The ABDM dashboard¹⁹⁸ provides some insights on the growth of the ecosystem and adoption. As of June 2026, over 926 million Ayushman Bharat Health Accounts (ABHAs) had been generated, covering nearly 65.5% of the population,^{199,200} compared to around 21% coverage in January 2023.²⁰¹ Similar gains have been observed in the onboarding of healthcare professionals and facilities, with over 40% of providers and a little over 50% of the facilities verified in 2025, up from less than 20% coverage across both registries in 2023.²⁰²

The cumulative linkage of health records has picked up pace in recent years, growing at a compound annual growth rate (CAGR) of 63.50% between 2022-23 and 2025-26, while

¹⁹⁹ Ayushman Bharat Digital Mission. (n.d.). *ABDM public dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/>

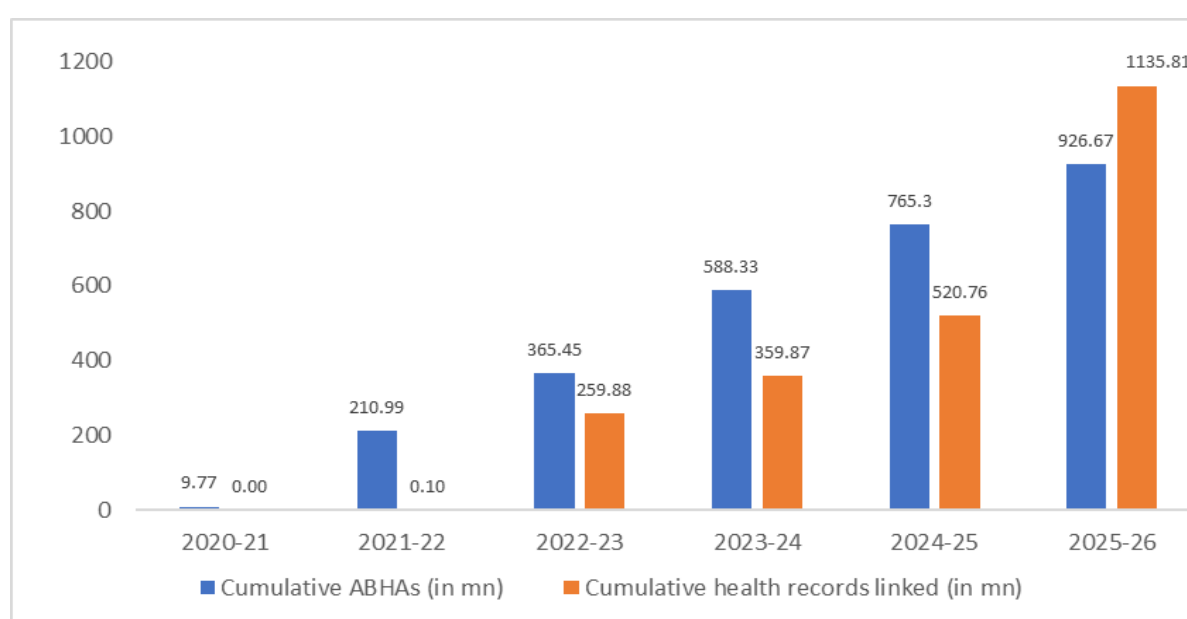
²⁰⁰ Saturation rate is calculated as a percentage of the 2022 population.

²⁰¹ Mishra, D., Kedia, M., Reddy, A., Kanwar, S., Manish, M., Das, B., Gupta, S., & Sharma, D. (2023). *State of India's digital economy report 2023*. Indian Council for Research on International Economic Relations (ICRIER). https://icrier.org/pdf/State_of_India_Digital_Economy_Report_2023.pdf

²⁰² Ayushman Bharat Digital Mission. (n.d.). *ABDM public dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/>

cumulative ABHA generation grew at a CAGR of 36.36% in the same period (Figure 8). This can mainly be attributed to the launch of the Digital Health Incentive Scheme (DHIS), which seeks to catalyse ABDM adoption among healthcare facilities and digital solution companies through providing monetary incentives based on the number of ABDM transactions conducted beyond a specified threshold.²⁰³ Of the total health records linked, only 0.02% have been linked by patients themselves, with the majority of the records linked by healthcare providers. Of the patients that have linked health records to their ABHA, less than 50% have linked more than one record.²⁰⁴ This suggests that the mission is currently driven predominantly by a supply-side push and will require concerted efforts to transition to a demand-pull model for long-term sustainability.

Figure 8: Cumulative Growth of ABHA Creation and Linkage of Health Records



Source: Authors' own, using ABDM Insights (2025-26 figures till 24 June 2026)

Since the initiation of the mission, the ABDM identities, registries and software have seen uneven diffusion across states as a result of regional variations in technological infrastructure and digital capabilities, financing, governance, capacity building and outreach, among others. Other important metrics include the utilisation of functionalities such as 'Scan-and-Share' and 'Scan-and-Pay' at ABDM-enabled facilities. As of June 2026, the Scan and Share feature aimed at streamlining Out Patient Department (OPD) registrations had recorded the issuance of 234.2 million tokens at 29,687 active health facilities. However, a large share of these tokens is being generated at a few public health facilities, particularly at various state branches of premier institutions such as the All India Institute of Medical Sciences (AIIMS), while only

²⁰³ National Health Authority. (n.d.). *Digital Health Incentive Scheme (DHIS)*. Government of India, Ayushman Bharat Digital Mission. <https://abdm-beta.abdm.gov.in/dhis>

²⁰⁴ Ayushman Bharat Digital Mission. (n.d.). *ABDM adoption dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/adoption>

around 1.6% of tokens are generated at private-sector hospitals.²⁰⁵ A similar pattern is observed in the Scan and Pay feature that was launched to streamline the payment process for tests, medicines and registrations.²⁰⁶

4.2 Technical Architecture

ABDM has a three-tiered technical framework (Figure 9). The first layer is the identification layer, which includes ABDM identities and registries that act as the definitive source of information on patients, healthcare professionals and facilities. The second layer is the gateways layer, which enables smooth health data exchange, service discovery and fulfilment within an interoperable network. The third layer consists of use case applications that integrate with the infrastructure to offer various services to patients, healthcare providers, insurers and others in the industry.

Figure 9: ABDM Technical Architecture



Source: Authors' own, based on ABDM roadmap²⁰⁷

An example of a process flow across the three layers can be demonstrated through the Scan-and Share functionality available in some ABDM-enabled facilities. During OPD registration, a patient creates ABHA (identity) through an ABDM-compliant Personal Health Record (PHR) application, scans the QR code at the ABDM-enabled facility and consents to sharing their details, such as name, gender and age. The details are routed through the Health Information Exchange (gateway) and sent to the Hospital Management Information System(application) of the provider.²⁰⁸ The gateways enable two-way exchange of information between participating entities through open APIs.

²⁰⁵ Ayushman Bharat Digital Mission. (n.d.). *ABDM Scan and Share dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/scanshare>

²⁰⁶ Ayushman Bharat Digital Mission. (n.d.). *ABDM Scan and Pay*. Government of India. <https://abdm.gov.in/scan-pay>

²⁰⁷ Ayushman Bharat Digital Mission. (n.d.). *Accelerating digitisation in healthcare delivery*. Government of India. https://abdm.gov.in/strapicms/uploads/Accelerating_Digitisation_in_Healthcare_Delivery_v3_fad6fe700f.pdf

²⁰⁸ Ayushman Bharat Digital Mission. (n.d.). *ABDM Scan and Share*. Government of India. <https://abdm.gov.in/scan-share>

A key ecosystem-enablement feature of ABDM is the sandbox environment, which allows developers and healthcare entities to build, test, validate and simulate ABDM integrations in a controlled non-production setting before deployment. This environment also supports API testing, interoperability validation and integration troubleshooting and accelerates onboarding and innovation across the ABDM ecosystem.²⁰⁹ However, several health-tech companies that integrated with ABDM in the sandbox environment reported initial challenges, including changing APIs and requirements at various milestones as well as server downtimes. Frequent API version updates without adequate deprecation windows have posed a significant barrier for smaller health IT vendors, some of whom have had to rebuild integrations multiple times.²¹⁰

One of the most significant core technological principles that underpin ABDM is the federated architecture that ensures that health records are stored at or closer to the point of care rather than in a centralised repository.²¹¹ With the scaling of the infrastructure in a large country, this principle has the advantage of reducing cost and redundancy arising from the duplication of storage and alleviating the risk of a single point of failure that could arise from the centralisation of large volumes of sensitive health data.²¹² The use of open APIs²¹³ as opposed to monolithic solutions reduces vendor lock-in and offers healthcare stakeholders the choice of a variety of applications through which to onboard ABDM and enables interoperability among systems. The adoption of a minimalistic approach²¹⁴ operationalised through minimised data collection in ABHA issuance and onboarding on registries, as well as Minimum Viable Product guidelines²¹⁵ for solution providers, offers the twin benefits of seeding the ecosystem with the opportunity for further incremental expansion while improving privacy and security.²¹⁶

4.2.1 Inclusivity in Design

“Design to be inclusive”, one of the core principles outlined in the National Digital Health Blueprint, highlights the need for specialised systems to be designed to “reach out to the “unconnected”, digitally illiterate, remote, hilly and tribal areas.”²¹⁷ The NHA has attempted

²⁰⁹ National Health Authority. (n.d.). *ABDM Sandbox*. Ayushman Bharat Digital Mission. <https://sandbox.abdm.gov.in/sandbox/v3>

²¹⁰ Stakeholder insights

²¹¹ National Institution for Transforming India (NITI Aayog). (2023). *NDHM strategy overview*. Government of India.

https://www.niti.gov.in/sites/default/files/2023-02/ndhm_strategy_overview.pdf

²¹² Balsari, S., Fortenko, A., Blaya, J. A., Gropper, A., Jayaram, M., Matthan, R., Sahasranam, R., Shankar, M., Sarbadhikari, S. N., Bierer, B. E., Mandl, K. D., Mehendale, S., & Khanna, T. (2018). Reimagining health data exchange: An application programming interface-enabled roadmap for India. *Journal of Medical Internet Research*, 20(7), e10725. <https://doi.org/10.2196/10725>

²¹³ Ministry of Health and Family Welfare. (2019). *National digital health blueprint*. Government of India.

https://abdm.gov.in/strapiCMS/uploads/ndhb_1_56ec695bc8.pdf

²¹⁴ Ministry of Health and Family Welfare. (2019). *National digital health blueprint*. Government of India.

https://abdm.gov.in/strapiCMS/uploads/ndhb_1_56ec695bc8.pdf

²¹⁵ Includes minimum mandatory features that an ABDM-enabled software must include. Ayushman Bharat Digital Mission. (n.d.). *Minimum Viable Product (MVP) guidelines 4.0*. Government of India.

https://abdm.gov.in/strapiCMS/uploads/MVP_Guidelines_4_0_476ab6be26.pdf

²¹⁶ Balsari, S., Fortenko, A., Blaya, J. A., Gropper, A., Jayaram, M., Matthan, R., Sahasranam, R., Shankar, M., Sarbadhikari, S. N., Bierer, B. E., Mandl, K. D., Mehendale, S., & Khanna, T. (2018). Reimagining health data exchange: An application programming interface-enabled roadmap for India. *Journal of Medical Internet Research*, 20(7), e10725. <https://www.imir.org/2018/7/e10725>

²¹⁷ Ministry of Health and Family Welfare. (2019). *National Digital Health Blueprint*. Government of India.

https://abdm.gov.in/strapiCMS/uploads/ndhb_1_56ec695bc8.pdf

to ensure inclusivity in the design of ABDM by making arrangements for the offline generation of ABHA in the paper-based mode and via digital devices for those with limited or no access to smartphones and internet connectivity.^{218,219} To enable non-smartphone users to avail the Scan-and Share facility, healthcare facilities have been advised to set up kiosks for the generation of physical ABHA cards, which still requires queuing but allows for the fetching of demographic details, thereby saving time in data entry.²²⁰

Initial learnings from the microsite project (discussed in section 4.3) that involved providing support to small clinics, hospitals and other facilities in onboarding ABDM revealed challenges such as patchy connectivity in remote areas and technical glitches in the deployment of ABDM-enabled software. A large share of these facilities also lacks prerequisite infrastructure such as hardware (laptops/computers) and digital storage capacity. For facilities that have already made such investments, there are complexities in integrating ABDM across various devices (smartphones, tablets and laptops) and systems (EHRs, administrative platforms) while ensuring a seamless experience for users of those digital solutions.²²¹ Some states have adopted various strategies to extend requisite telecom and internet connectivity infrastructure as well as backup offline processes to support ABDM adoption at the facility level, such as offering free Wi-Fi facilities for patients at some health facilities, partnering with multiple internet service providers to maintain stable connectivity at various levels of care, enabling offline data capture in ABDM-enabled HMIS software and equipping frontline healthcare functionaries with smartphones and tablets pre-loaded with ABDM-enabled applications with the capability of operating in low bandwidth, among other measures.²²²

The ABDM portal ensures accessibility for visually impaired individuals through assistive technologies such as screen readers.²²³ However, there is no requirement for private applications onboarding the infrastructure to adhere to accessibility guidelines. Although the Rights of Persons with Disabilities Act, 2016, lays down certain obligations for digital accessibility,²²⁴ compliance from digital platforms has been limited.²²⁵

The extent to which a participative design process for interfaces such as the ABHA app and other touchpoints for ABDM interactions has considered specific accessibility barriers and

²¹⁸ Ayushman Bharat Digital Mission. (n.d.). *Guidelines for offline ABHA generation using digital devices*. Government of India. [https://abdm.gov.in/strapicms/uploads/Guidelines Offline ABHA generation using digital devices 023a71b9cc.pdf](https://abdm.gov.in/strapicms/uploads/Guidelines%20Offline%20ABHA%20generation%20using%20digital%20devices%20023a71b9cc.pdf)

²¹⁹ Ayushman Bharat Digital Mission. (n.d.). *Guidelines for offline ABHA generation using paper-based data collection*. Government of India. [https://abdm.gov.in/strapicms/uploads/Guidelines for Offline ABHA generation using paper based data collection 1c08421ca5.pdf](https://abdm.gov.in/strapicms/uploads/Guidelines%20for%20Offline%20ABHA%20generation%20using%20paper%20based%20data%20collection%201c08421ca5.pdf)

²²⁰ Ayushman Bharat Digital Mission. (2023). *ABDM Scan and Share onboarding manual*. Government of India. [https://abdm.gov.in/strapicms/uploads/ABDM Scan and Share Onboarding Manual 18_01_2023_1_0600fe7747.pdf](https://abdm.gov.in/strapicms/uploads/ABDM%20Scan%20and%20Share%20Onboarding%20Manual%2018_01_2023_1_0600fe7747.pdf)

²²¹ Research and Innovation Circle of Hyderabad. (n.d.). *Ayushman Bharat Digital Mission (ABDM) report*. Government of Telangana. <https://rich.telangana.gov.in/assets/pdfs/Reports/ABDM-Report.pdf>

²²² Ayushman Bharat Digital Mission. (2025). *State best practices 2024–25*. Government of India. [https://abdm.gov.in/strapicms/uploads/State Best Practices 2024_25_f2785577de.pdf](https://abdm.gov.in/strapicms/uploads/State%20Best%20Practices%202024%2025_f2785577de.pdf)

²²³ Ayushman Bharat Digital Mission. (n.d.). *Screen reader access*. Government of India. <https://abdm.gov.in/screen-reader-access>

²²⁴ Iqbal, S. (2025, June 13). *RPwD Act and IS 17802: India's digital accessibility standards (2025 guide)*. Pivotal Accessibility. <https://www.pivotalaccessibility.com/2025/06/rpwd-act-and-is-17802-indias-digital-accessibility-standards-2025-guide/>

²²⁵ Sharma, N. (2025, August 1). *Digital access as a fundamental right*. Vidhi Centre for Legal Policy. <https://vidhilegalpolicy.in/blog/digital-access-as-a-fundamental-right/>

concerns for marginalised communities such as women and people with disabilities is also uncertain. ABHA generation among men and women is roughly equally distributed,²²⁶ but inclusive design considerations need to move beyond adoption numbers to support active usage. Amid persistent systemic gender divides in device ownership, connectivity and digital literacy,²²⁷ even urban educated women have reported reluctance in use of digital health applications due to lack of trust and complexity in navigation, among other factors.²²⁸ Among economically weaker segments, sustained use of ABDM applications is constrained by costly data plans and expensive recharges.²²⁹ These multifaceted barriers across demographic groups need to be addressed for scaling meaningful access to the infrastructure.

Thus, ABDM exhibits mixed performance under the accessibility and inclusivity pillar of the evaluative framework, with varying progress in terms of gender inclusion, disability access and geographic coverage among other elements.

4.2.2 Limitations of the Architecture

Beyond challenges of meaningful access, other limitations arise from the underlying design and architecture. ABHA can be generated through multiple pathways, including Aadhaar-based authentication, driving licence-based registration and offline-assisted workflows. While Aadhaar-enabled onboarding improves convenience and de-duplication, it also raises important concerns regarding the linkage of health data with a biometric-backed national identity system, necessitating stronger safeguards around privacy, consent, exclusion prevention and proportionality of data usage. Offline ABHA creation addresses onboarding barriers at the identity layer but does not adequately resolve broader digital exclusion related to transactional participation in the ABDM ecosystem.

Scholars have argued that, alongside its benefits, the federated architecture brings certain challenges, such as resource-intensive maintenance, coordination failure in case of the absence of any participant in the node, and complexity in scaling changes across the ecosystem.²³⁰ Moreover, the complexity of Fast Healthcare Interoperability Resources (FHIR) implementation has meant that, in the absence of standardised coded clinical data using semantic terminologies, the ecosystem's ability to support computable interoperability, advanced analytics, clinical decision support and longitudinal population health intelligence remains constrained. Certain stakeholders have also reported incomplete health records being linked to the unique health ID, which impacted the usability of those records for healthcare professionals and impacted M3 (exchange of health records) adoption at the early

²²⁶ Ayushman Bharat Digital Mission. (n.d.). *ABDM public dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/>

²²⁷ Khan, S., & Bhatia, R. (2023). *Digital dreams, gendered realities: Women in digital India*. Centre for Economic Data and Analysis (CEDA), Ashoka University. <https://ceda.ashoka.edu.in/digital-dreams-gendered-realities-women-in-digital-india/>

²²⁸ Pasumarthi, B. (2024, June 4). *Towards a gender-inclusive digital health system in India*. International Innovation Corps, University of Chicago. <https://www.iic.uchicago.edu/blog/towards-a-gender-inclusive-digital-health-system-in-india>

²²⁹ Ranjan, A., Singh, G., Singh, H., & Singh, M. (2026). Adoption, digital health literacy, and patient satisfaction of Ayushman Bharat Digital Mission: An analytical cross-sectional study among outpatient department attendees. *BMC Health Services Research*, 26, 512. <https://link.springer.com/article/10.1186/s12913-026-14314-7>

²³⁰ Mantri, M., Sunder, G., Kadam, S., & Abhyankar, A. (2024). A perspective on digital health platform design and its implementation at national level. *Frontiers in Digital Health*, 6, 1260855. <https://doi.org/10.3389/fdgth.2024.1260855>

stages of ABDM. Prioritising data completeness and accuracy in the linking and exchange of health records is essential for minimising chances of misinterpretation of patient information and ensuring quality care and patient safety.^{231,232}

There are other operational challenges concerning the technical architecture. Several health facilities have multiple and fragmented legacy healthcare IT systems that cannot seamlessly communicate with ABDM APIs and require custom integration, which results in additional cost and effort. Certain states may have been forced to replace their existing open-source systems with centralised ABDM-compliant solutions, disrupting long-term relationships with implementing agencies critical for technical capacity-building and the sustainability of digitalisation initiatives at healthcare facilities.²³³ Additionally, while healthcare providers may be keen on adopting digital tools, existing systems are often designed around administrative or reporting needs rather than aiding clinicians in their workflows, which has implications for the adoption of provider-facing applications that integrate with the mission.

It is also unclear how registries are capturing dynamic attributes; while details such as the name and ID of facilities in the HFR are static, details about the upgradation of facilities and services or the shutting down of facilities change over time. Another prominent question pertains to the interoperability of registries with existing databases and whether lessons learned from previous attempts at building repositories (such as challenges in the categorisation of facilities) were incorporated in the design of the ABDM registries. Several registry-related indicators provided by the dashboard require cautious interpretation due to inconsistencies in legacy databases, duplicate facility entries, outdated baselines and variable verification methodologies across states.^{234,235}

4.3 Governance

Aligning the interests of multiple stakeholders necessitates a balance between centralised strategic oversight and sufficient operational flexibility. Structured mechanisms exist in the form of official guidelines, standard operating procedures (such as those for verification of health facilities and healthcare professionals) and reviews that enable the coordination of activities at various levels, including the district level. However, the ABDM has developed in a legislative vacuum, and gaps remain in transparency and grievance redressal. This section examines how the ABDM infrastructure fares in terms of legislative and regulatory compliance, transparency and accountability, and user communication from the evaluative framework.

²³¹ Stakeholder insights.

²³² Research and Innovation Circle of Hyderabad. (n.d.). *Ayushman Bharat Digital Mission (ABDM) report*. Government of Telangana. <https://rich.telangana.gov.in/assets/pdfs/Reports/ABDM-Report.pdf>

²³³ RTH Resources. (2023, September 14). *Digitization of health services – Part I: Decoding the Ayushman Bharat Digital Mission (ABDM)*. <https://rthresources.in/conversations-on-health-policy/digitization-of-health-services-part-i-decoding-the-ayushman-bharat-digital-mission-abdm/>

²³⁴ National Health Authority. (2026, January 29). *Digital health innovations in India | StateXchange | Digital health best practices & cross-learning* [Video]. YouTube. <https://www.youtube.com/watch?v=u5pjFF9TgCA>

²³⁵ Stakeholder insights.

4.3.1 Decentralised Governance and Multi-Stakeholder Coordination

The multi-layered governance structure of the ABDM consists of public and private stakeholders at various levels – national, state and district. The roles and responsibilities at these levels, mapped in the ABDM handbook,²³⁶ are presented in Appendix 3. The strategic guidance of the mission is provided by the National Health Authority (NHA), an apex body situated within the Ministry of Health and Family Welfare, while implementation is largely decentralised at the state and district levels. This decentralisation has resulted not only in fragmentation of outcomes but also in processes such as the verification of facilities²³⁷ as well as establishment or lack of dedicated state ABDM websites.²³⁸

Operational coordination of the NHA with states has been institutionalised in the form of recurring trainings and workshops with select state and Union Territory officials,^{239,240} national and regional review meetings for stocktaking on progress and challenges^{241,242} and promotion of cross-state knowledge exchange on best practices through events,²⁴³ documents²⁴⁴ and virtual platforms.²⁴⁵ Such mechanisms serve as a two-way feedback system for states to incorporate the NHA's directions to address gaps in planning and implementation and for the national authority to iterate on strategy and guidelines.

The microsite²⁴⁶ initiative is an example of innovative, broad-based participative governance aimed at aligning diverse stakeholders around a common objective. The project was conceptualised as a partnership between the NHA and state ABDM offices in the health tech sector and in not-for-profit organisations.²⁴⁷ The roles and responsibilities have been clearly delineated for smoother coordination across the activity chain, along with operational guidelines for project financing and implementation²⁴⁸ (Figure 10).

²³⁶ Ayushman Bharat Digital Mission. (n.d.). *ABDM e-book*. Government of India. <https://abdm.gov.in/ebook>

²³⁷ Ayushman Bharat Digital Mission. (n.d.). *ABDM public dashboard*. Government of India. <https://dashboard.abdm.gov.in/abdm/>

²³⁸ While some states such as Uttar Pradesh and Jharkhand have separate ABDM portals, most other states do not.

²³⁹ Ministry of Health and Family Welfare. (2022, June 8). *National Health Authority (NHA) organizes orientation workshop for Joint Directors/Directors of State on Ayushman Bharat Digital Mission (ABDM) in Mumbai*. Press Information Bureau, Government of India. <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1832106>

²⁴⁰ National Health Authority. (n.d.). *Training and workshop*. Ayushman Bharat Digital Mission. <https://abdm.gov.in/training-and-workshop>

²⁴¹ Ministry of Health and Family Welfare. (2025, October 16). *National Health Authority Hosts 2-Day PM-JAY & ABDM National Review Meeting in Bhopal, Madhya Pradesh*. Press Information Bureau, Government of India. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2179797>

²⁴² Ministry of Health and Family Welfare. (2022, July 2). *National Health Authority (NHA) organised Western Region Review Meeting in Pune, Maharashtra to assess implementation progress and draw future roadmap for Ayushman Bharat PM-JAY & Ayushman Bharat Digital Mission (ABDM) schemes across the region*. Press Information Bureau, Government of India. <https://www.pib.gov.in/PressReleaselframePage.aspx?PRID=1838800>

²⁴³ National Health Authority. (n.d.). *Final booklet design (single read)*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapicms/uploads/FINAL_Booklet_Design_single_read_6a4898a934.pdf

²⁴⁴ National Health Authority. (n.d.). *ABDM best practices (redesigned)*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapicms/uploads/ABDM_Best_Practices_Reddesigned_63461c1e9d.pdf

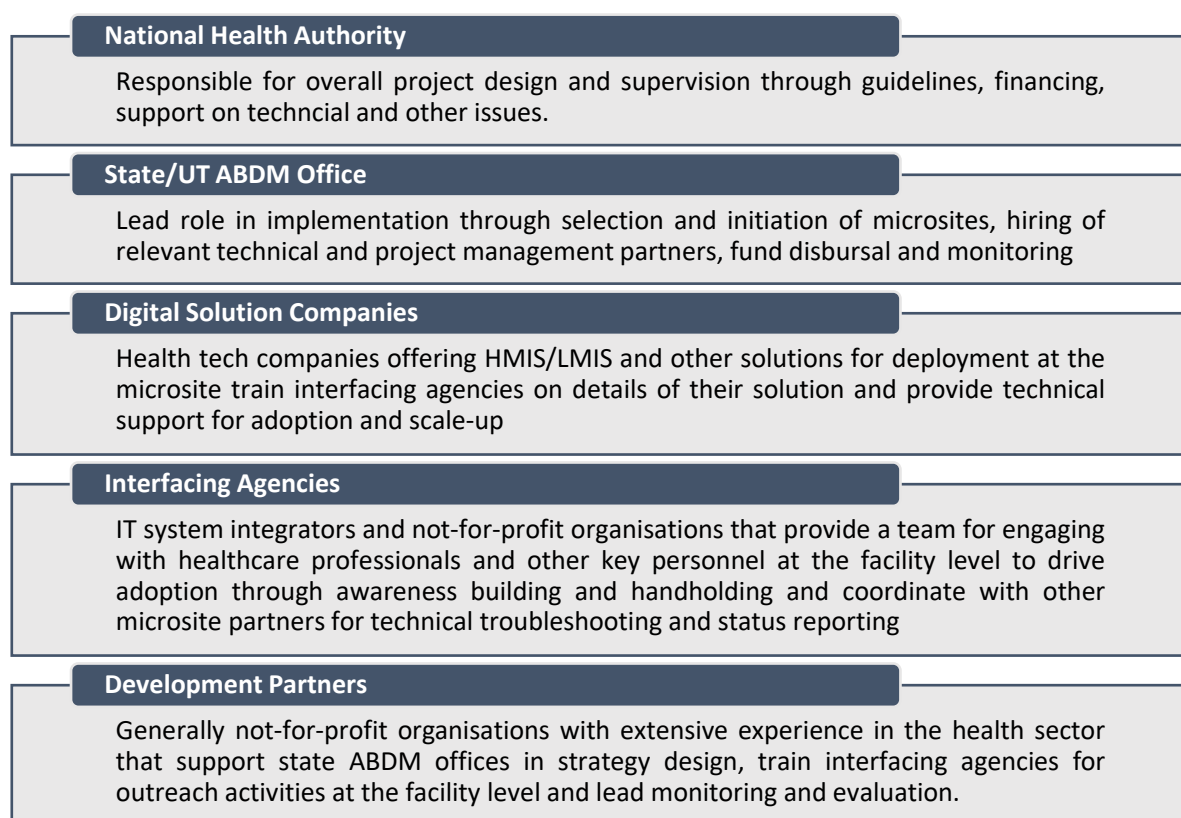
²⁴⁵ National Health Authority. (n.d.). AyushmanNHA [YouTube channel]. YouTube. <https://www.youtube.com/@AyushmnaNHA>

²⁴⁶ A microsite is a “focused region comprising of all small-medium sized healthcare facilities such as clinics, hospitals, labs, pharmacies within that area, which may be onboarded onto the ABDM ecosystem.” <https://abdm.gov.in/microsites>

²⁴⁷ National Health Authority. (n.d.). *Partners*. Ayushman Bharat Digital Mission. <https://abdm.gov.in/microsites/partners>

²⁴⁸ National Health Authority. (n.d.). *Operational guidelines for ABDM*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapicms/uploads/operational_Guidelines_9d3cf828f4.pdf

Figure 10: Multi-Stakeholder Coordination in the 100 Microsite Project



Source: Authors' own, developed from *Microsite Operational Guidelines*²⁴⁹

This model has had considerable success in expediting adoption. As of June 2026, 124 active microsites had registered over 78,000 healthcare professionals on the HPR and over 66,000 facilities on the HFR, with over 21,000 of them using ABDM-enabled solutions and linking over 16 million records.²⁵⁰ Cluster-based rollout generates network effects within targeted sites by building peer pressure among facilities and creating momentum for further scale-up. The strategy of pooling resources through sharing IT systems and funding and training personnel across multiple facilities creates economies of scale. The public-private partnership model also enables building trust with small- and mid-sized facilities in the unorganised healthcare sector and accelerates learning through rapid feedback loops that inform future course of action.²⁵¹

However, this model also presents complexities. Experiences from certain states indicate that multiple reporting lines have complicated coordination among stakeholders, resulting in a lack of ownership of outcomes and setting perverse incentives for chasing quantitative targets rather than focusing on the quality of the data in linked records.²⁵² Moreover, horizontal

²⁴⁹ National Health Authority. (n.d.). *Additional CEO letter and microsite guidelines*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapicms/uploads/Addl_CEO_letter_and_Microsite_Guidelines_7d16822da9_8dc7431637_3e4e882ad8.pdf

²⁵⁰ National Health Authority. (n.d.). *Microsite dashboard*. Ayushman Bharat Digital Mission. <https://dashboard.abdm.gov.in/abdm/microsite>

²⁵¹ Stakeholder insights.

²⁵² Stakeholder insights.

coordination across ministries and the enforcement of aligning state legacy systems with ABDM standards through vertical coordination continue to remain uneven.²⁵³

Beyond coordination complexities, a key issue behind the low uptake of the ABDM has been the misalignment of incentives among stakeholders.²⁵⁴ UPI's success in fintech can be partly attributed to direct benefits and the convergence of incentives for users, payment apps, merchants and banks. However, most entities in the healthcare ecosystem face substantial immediate costs for participating in the digital health mission in terms of investments in hardware, integration of existing systems and staff training, among others, with limited and uncertain future returns. There are also conflicting incentives; while patients gain from longitudinal records and portability, healthcare providers apprehend the loss of patients, increased regulatory scrutiny and taxation.²⁵⁵ Similarly, while a standardised gateway for health insurance seeks to solve for inefficient processes in the existing claims settlement system that affect both parties,²⁵⁶ it is also expected to reduce pricing flexibility for providers, create greater transparency and shift bargaining power in favour of insurers and patients.²⁵⁷

4.3.2 Policy Foundations and Health Data Governance

The National Health Policy 2017 provided for the establishment of a National Digital Health Agency “to regulate, develop and deploy digital health across the continuum of care,” creation of a federated national health information architecture, registries and health information exchange, among others.²⁵⁸ Subsequently, the National Health Stack,²⁵⁹ the National Digital Health Blueprint²⁶⁰ and the National Digital Health Mission Strategy²⁶¹ documents elaborated on the technical architecture, institutional mechanisms and standards, including those for preserving health data privacy and security, as well as legal and regulatory requirements for IT systems envisaged under the ABDM (Figure 11). Health data governance under the ABDM is primarily guided by the Health Data Management Policy, 2020, and the Digital Personal Data Protection (DPDP) Act, 2023.

²⁵³ Kadambi, P., Joseph, P. T., & Ajitsaria, D. (2025). *Ayushman Bharat Digital Mission: From infrastructure to impact—A tri-lens assessment of India's digital health system*. Figshare. <https://doi.org/10.6084/m9.figshare.30971167>

²⁵⁴ Das, B., & Khan, M. (2026, April). *Economics of DPI in healthcare: Catalysing digital health innovation through ABDM* (Policy Brief No. 11). Indian Council for Research on International Economic Relations (ICRIER). <https://icrier.org/pdf/Economics-of-DPI-inHealthcare.pdf>

²⁵⁵ Medical Buyer. (2025, February 12). *Many healthcare providers fear accountability, not accepting digital health records*. <https://medicalbuyer.co.in/many-healthcare-providers-fear-accountability-not-accepting-digital-health-records/>

²⁵⁶ NATHEALTH. (2025). *National Health Claims Exchange: The next step in digital health interoperability*. https://nathealthindia.org/wp-content/uploads/2025/06/National-Health-Claims-Exchange_Latest.pdf

²⁵⁷ Ohri, N. (2025, July 10). India plans to tighten oversight of claims portal to curb rising healthcare costs, source says. *Reuters*. <https://www.reuters.com/business/healthcare-pharmaceuticals/india-plans-tighten-oversight-claims-portal-curb-rising-healthcare-costs-source-2025-07-10/>

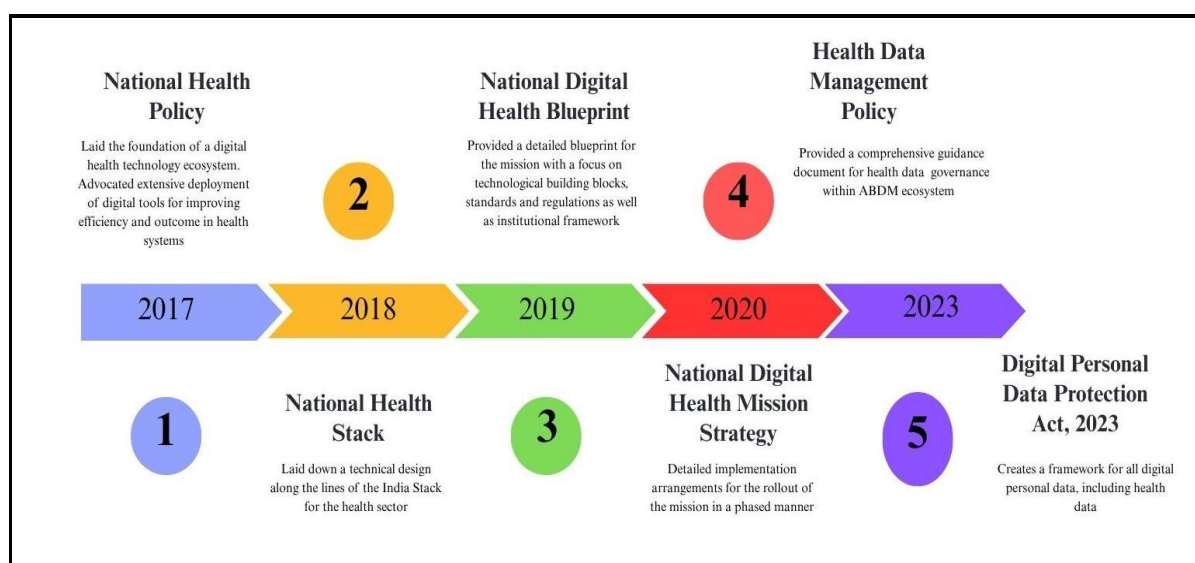
²⁵⁸ Ministry of Health and Family Welfare. (2017). *National Health Policy 2017*. Government of India. <https://nhsrcindia.org/sites/default/files/2021-07/National%20Health%20Policy%202017%20%28English%29%20.pdf>

²⁵⁹ NITI Aayog. (2018, July). *National Health Stack: Strategy and approach*. Government of India. https://abdm.gov.in/strapicms/uploads/NHS_Strategy_and_Approach_1_89e2dd8f87.pdf

²⁶⁰ Ministry of Health and Family Welfare. (2019). *National Digital Health Blueprint*. Government of India. https://abdm.gov.in/strapicms/uploads/ndhb_1_56ec695bc8.pdf

²⁶¹ National Health Authority. (2020, July). *National Digital Health Mission: Strategy overview—Making India a digital health nation: Enabling digital healthcare for all*. Government of India. https://www.niti.gov.in/sites/default/files/2023-02/ndhm_strategy_overview.pdf

Figure 11: Evolution of the Policy and Governance Framework of ABDM



Source: Authors' own, from secondary sources

Several critics have pointed to the rapid advancement in the digital health ecosystem in the midst of fragmented regulations and absence of an overarching primary legislation backing the creation of the mission and the governance of health data.^{262,263} The use of executive policies over legislative frameworks has implications such as provisions of the policies being non-justiciable²⁶⁴ and procedural drawbacks such as inadequate time for public consultations and feedback.²⁶⁵

While the sector-specific legislation, the Digital Information Security in Healthcare Act (DISHA),²⁶⁶ which clearly defined health data, ownership and rights as well as institutions and processes for management and security of health data, was initially proposed in 2018, it was later abandoned. Unlike the financial and telecommunications sectors, which are governed by specialised regulatory authorities with enforcement powers, the digital health ecosystem lacks an institution exclusively responsible for the oversight of health data governance, interoperability compliance, cybersecurity accountability and privacy enforcement. This creates a governance gap within the ABDM ecosystem, particularly given the highly sensitive nature of longitudinal health data and the increasing scale of digital health transactions.²⁶⁷

²⁶² Garg, O., Choksi, M., & Mokashi, T. (2025). *Strengthening health governance and data protection through the Digital Data Protection Act, 2023 in India's digital health ecosystem* [Poster]. PMAC 2025. <https://pmac-2025.com/uploads/poster/A089-OSHIAGARG-6635.pdf>

²⁶³ Chandrasekhar, R. (2024). Datafication, power, and publics in India's national digital health ecosystem. *Social Science Research Network (SSRN)*. <https://ssrn.com/abstract=4981374>

²⁶⁴ Centre for Internet and Society. (2022). Deployment of digital health policies and technologies. <https://cis-india.org/internet-governance/deployment-of-digital-health-policies-and-technologies>

²⁶⁵ Chandrasekhar, R. (2024). Datafication, power, and publics in India's national digital health ecosystem. *Social Science Research Network (SSRN)*. <https://ssrn.com/abstract=4981374>

²⁶⁶ Ministry of Health and Family Welfare. (2018). *Draft Digital Information Security in Healthcare Act (DISHA)*. Government of India. <https://dn720701.ca.archive.org/0/items/draftdishaact/draft%20Disha%20Act.pdf>

²⁶⁷ The Centre for Internet and Society. (2023, February 6). *Do we need separate health data laws in India?* <https://cis-india.org/internet-governance/do-we-need-separate-health-data-india.pdf>

The prevailing DPDP Act makes no distinction between sensitive personal data and personal data and leaves a gap in legal recourse and accountability, as it does not specify compensation models for those affected by data breaches.²⁶⁸ Moreover, while the ABDM's privacy architecture is largely consent-based, the DPDP Act permits the processing of personal data without explicit consent for certain public health and state functions such as disease surveillance, epidemic response and government programme monitoring. This creates an important governance consideration for the use of ABDM-linked data in public health and highlights the need for clear safeguards and accountability mechanisms.²⁶⁹

4.3.3 Grievance Redressal

ABDM has established a detailed redressal mechanism for registering grievances of various stakeholders in the ecosystem. Aggrieved parties can register their complaints through various channels – the web portal available in English, call centre support available in six languages on a toll-free number and postal letters at a specified address.²⁷⁰ The NHA has signed a Memorandum of Understanding (MoU) with Digital India BHASHINI Division²⁷¹ to enable multilingual translation services and AI-powered language support that would be deployed across citizen-facing interfaces for inclusive reach of these mechanisms among other use cases.²⁷² The grievance portal also provides a tab for tracking registered complaints, submitting feedback/suggestions on the various components of the mission and has a detailed FAQ for common queries of stakeholders. A three-level institutional structure for handling complaints, with descriptions of their functions, stipulated turnaround time (TAT) for resolution by each team, grievance workflow and an escalation matrix for government integrators is publicly available²⁷³ but has not been incorporated in the grievance portal. While the prescribed turnaround time for resolution is 30 days,²⁷⁴ there is no reporting of metrics on the dashboard on the number and types of complaints registered and actual average TAT. The ABDM sandbox has a separate portal for digital solution companies and other integrators to raise technical issues during integration.²⁷⁵ While the turnaround time for ticket resolution is generally 24 hours for common and minor queries, certain technology partners have reported delays in more complex, recurring issues.²⁷⁶

²⁶⁸ Research and Innovation Circle of Hyderabad. (2025). *Digital personal data protection (DPDP) Act, cybersecurity, and real-world practices for healthcare*. Government of Telangana. <https://rich.telangana.gov.in/assets/pdfs/Reports/DPDP-Act-Cybersecurity-and-Real-World-Practices-for-Healthcare.pdf>

²⁶⁹ Stakeholder Insights

²⁷⁰ National Health Authority. (n.d.). *About grievance portal*. Ayushman Bharat Digital Mission. <https://grievance.abdm.gov.in/grievance/v3/about-us>

²⁷¹ Ministry of Electronics and Information Technology. (n.d.). *Bhashini: National language translation mission*. Government of India. <https://bhashini.gov.in/>

²⁷² Ministry of Electronics & IT. (2026, January 19). *Signing of Memorandum of Understanding (MoU) between Digital India BHASHINI Division and National Health Authority*. Government of India. <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2216227®=3&lang=1>

²⁷³ National Health Authority. (n.d.). *Grievance redressal system user guide (v2)*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapi/cms/uploads/Grievance_v2_90dd9b1ade_b0602176ca.pdf

²⁷⁴ National Health Authority. (n.d.). *Frequently asked questions (FAQ)*. Ayushman Bharat Digital Mission grievance portal. <https://grievance.abdm.gov.in/grievance/v3/faq>

²⁷⁵ National Health Authority. (n.d.). *ABDM sandbox support*. Ayushman Bharat Digital Mission. <https://sandboxsupport.abdm.gov.in/index.php>

²⁷⁶ Stakeholder insights.

4.4 Efficiency

Since the inception of the digital health mission, there has not been a systematic impact assessment of the overall outcomes. Some insights gained from official documents and stakeholders indicate efficiency gains for patients, healthcare providers and administrators, as well as innovation and market opportunities for health tech businesses. In particular, the mission's most visible impacts are aligned with the process optimisation and innovation factors identified in the evaluative framework.

- **Streamlined patient registration:** In terms of efficiency gains, one of the most evident impacts of the mission is through the scan-and-share facility, which has streamlined OPD registration by enabling digital capturing and sharing of demographic details from ABHA and the records linked to it to the health facility's HMIS. This has helped solve the twin problem of long queues and extended waiting time for patients at registration as well as manual data-entry errors by operators. Besides saving an estimated 30 minutes,²⁷⁷ it has reduced wages lost.
- **Better continuity of care:** Some healthcare providers in tertiary care facilities that are implementing ABDM are already reporting benefits in clinical decision-making through the availability of longitudinal records such as reports, discharge summaries and operative notes. This has been particularly helpful in ensuring smoother referrals, reducing the need for repeated history taking and testing, identifying misdiagnoses, timely course correction and improving patient safety and care, particularly in emergency cases.²⁷⁸
- **Enabling operational efficiencies for small and medium clinics:** The mission is also playing an instrumental role in nudging digitalisation and optimising patient journeys and workflows in many small and medium private clinics that previously had low digital maturity and largely relied on paper-based systems. This is being done through the two-pronged approach of rolling out lightweight and low-cost solutions developed by the public sector²⁷⁹ as well as through subsidising the cost of adopting ABDM-enabled health tech offerings from the private sector.
- **Improving insurance claims processing efficiency through NHCX:** Another emerging area of impact within the ABDM ecosystem is the National Health Claims Exchange (NHCX), which aims to standardise and digitise insurance claims processing across insurers, hospitals, Third Party Administrators (TPAs) and government schemes. By enabling interoperable and machine-readable claims exchange through a unified protocol, the NHCX seeks to reduce fragmented workflows, manual paperwork and long

²⁷⁷ Ministry of Health and Family Welfare. (2024). *Ayushman Bharat Digital Mission marks a transformative three-year journey towards enabling digital health* [Press release]. Press Information Bureau.
<https://www.pib.gov.in/PressReleaseFramePage.aspx?PRID=2059537®=3&lang=2>

²⁷⁸ Roundtable stakeholder insights.

²⁷⁹ Ministry of Health and Family Welfare. (2025). National Health Authority and C-DAC Sign MoU to roll out a light HMIS for Digitization of Small and Medium Healthcare Providers. Press Information Bureau.
<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2156603®=3&lang=2>

reimbursement timelines that traditionally extend to several weeks. Although ecosystem-wide adoption is still evolving, NHCX represents an important step towards improving transparency, administrative efficiency and digital health financing infrastructure in India.

- **Innovation enablement:** The ABDM is also helping health tech companies build innovative services on top of building blocks. Certain startups are expanding beyond their core portfolio of services by developing simplified plug-and-play API suites called connectors to enable the seamless integration of existing health IT systems and applications with the ABDM. Some other innovative use cases include health tech companies leveraging AI to convert unstructured data to FHIR-aligned formats and the use of ABDM components for fraud detection and efficient management of insurance claims.²⁸⁰

4.5 Privacy and Security

Privacy and security constitute two important dimensions for building trust within the DPI-H ecosystem. Central to the privacy concern is the fear of individuals losing control over their information and the harms resulting from the unpredictable use of data by unknown entities for purposes such as profiling for commercial interests, predatory targeting and unfair scoring for insurance, as well as data leakages, which can result in social prejudice and discrimination.²⁸¹ Additionally, growing data breaches from technical vulnerabilities, malicious insider threats and third-party failures from vendors and human error, coupled with the high value of medical records in underground markets, underscores the urgent need for strong data protection measures for building confidence among stakeholders.²⁸² This section examines elements of privacy, data protection and cybersecurity through the evaluative framework.

4.5.1 Privacy by Design

One of the core principles adopted in the blueprint of the national digital health mission is “ensuring security and privacy by design.” To operationalise this principle, the Health Data Management Policy (HDMP) provides guidance on the protection of individuals’ digital health data privacy, covering aspects such as consent framework, policy for allocation of various identities and obligation of data fiduciaries.

This policy, in conjunction with the DPDP Act, provides the privacy and security framework for health data in the ecosystem. Both emphasise the principles of data minimisation, purpose limitation and storage limitation. Data minimisation in the technical architecture is embedded by collecting only the minimum personal data required for creating specific identities. For

²⁸⁰ National Health Authority. (n.d.). *ABDM winners presentation*. Government of India, Ayushman Bharat Digital Mission. https://abdm.gov.in/strapi/cms/uploads/Winners_PPT_888936df1a.pdf

²⁸¹ Agrawal, P., Sharma, S., Sagar, A., & Banerjee, S. (2023). On health data architecture design. In S. Parsheera (Ed.), *Private and controversial: When public health and privacy meet in India*. HarperCollins India.

²⁸² Research and Innovation Circle of Hyderabad. (2025). *Digital personal data protection (DPDP) Act, cybersecurity, and real-world practices for healthcare*. Government of Telangana. <https://rich.telangana.gov.in/assets/pdfs/Reports/DPDP-Act-Cybersecurity-and-Real-World-Practices-for-Healthcare.pdf>

instance, ABHA generation requires only basic demographic details, such as name, year of birth or age, gender and mobile number. Similarly, the Health Professional ID requires a limited set of additional information, such as professional qualifications, location of practice and registration details, while other checks and verifications are carried out through existing information in the databases of regulatory bodies.

The HDMP sets out the general principles governing the ABDM consent framework, conditions for validity of consent and methods for obtaining consent respectively. The data principal is vested with control and decision-making power over the manner of collection and the processing of his/her personal data, and the policy lays down essential requirements for technical design of the consent framework, specifically the use of secure technologies for preventing breaches, guaranteeing the integrity of access permissions and ensuring interoperability of the consent management framework across all players in the ecosystem. Consent in the ABDM technical architecture is aligned with the MeitY electronic consent framework,²⁸³ which recognises “user-centricity” and “granular control” as two key design principles. At the core of this architecture is the consent artefact – a machine-readable electronic document specifying the parameters and scope of data share that a user consents to in an ABDM data-sharing transaction. Some key attributes of this consent artefact, which allows multi-dimensional granular control for the patient, are presented in Table 8.

Table 8: Key Attributes of the Consent Artefact

Dimensions of consent	Description
Purpose of Use	Defines the purpose of the request, such as care management and public health.
Health Information Types	Defines the type of information requested, such as prescription, diagnostic report and discharge summary.
Requester	Specifies the entity requesting the data, i.e., name of the hospital, doctor, etc.
Range	Specifies the time period of health records that can be accessed.
Validity	Specifies the consent duration.

Source: ABDM Sandbox documentation²⁸⁴

The revocability of consent is also recognised within the HDMP. The policy provides for the deemed revocation of consent to accessing health records linked to a health ID that has been deactivated by the data principal. While the consent flow in the developer documentation mentions other aspects of consent, these are generally not available in patient-facing applications, as some of these aspects are extremely granular and technically complex.

²⁸³ Ministry of Electronics and Information Technology. (2020). *Electronic consent framework (version 1.1): Technology specifications*. Digital Locker Authority. <https://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf>

²⁸⁴ National Health Authority. (n.d.). *Getting started: ABDM sandbox documentation (v3)*. Ayushman Bharat Digital Mission. <https://sandbox.abdm.gov.in/sandbox/v3/new-documentation?doc=getting-started>

Weak privacy policies in the health application ecosystem remain a concern. A key aspect of the HDMP is the requirement for data fiduciaries to provide a clear privacy notice to data principals. Several studies have pointed to citizens' concerns around data privacy and security as one of the main barriers to adoption of digital health and ABDM.²⁸⁵ In an independent evaluation of the privacy policies of commonly used health applications in the ABDM ecosystem, many applications, with the exception of the ABHA app, scored low or moderate on common principles of data protection. Private health tech applications fared particularly low on the plain language readability of their privacy notices. Moreover, none of the examined applications had privacy policies available in regional languages, and users had to either consent to all the policies of the app or stop using their services.²⁸⁶

With regard to data retention, the NHA's consultation paper on health data retention policy prescribed a minimum retention period of 10 years for in-patient, outpatient and deceased patients after the last appointment, with the exception of medico-legal documents, immunisation records, clinical trials and, birth and death registrations.²⁸⁷ However, the policy has not been finalised. In practice, data retention schedules across healthcare facilities in the country are staggered and determined by self-prescribed standards at the facility level meant to cover compliance requirements across various existing regulations and guidelines such as the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, the Clinical Establishments (Registration and Regulation) Draft Rules, 2010, and the Office Memorandum of the Directorate General of Health Services for Central Government Hospitals in 2014, among others.²⁸⁸

With regard to data deletion, the HDMP requires data fiduciaries to delete personal data after the purpose for which it was collected and processed has been served, with the exception that data may be retained for longer periods subject to the consent of the data principal and if such retention is necessary for the fulfilment of obligations under any applicable law.²⁸⁹

Offline modes of ABHA creation have several physical touchpoints and manual interactions that raise privacy risks. While guidelines prescribe detailed procedures for the collection and handling of personal data in these modes, there is limited clarity on how compliance is enforced. In particular, the scope of ABDM audit mechanisms for ensuring adherence to the minimum standards on data security and safety and deletion of records are not clearly codified, and timelines seem largely discretionary. Ambiguities also exist around procedures

²⁸⁵ Ranjan, A., Singh, G., Singh, H., & Singh, M. (2026). Adoption, digital health literacy, and patient satisfaction of Ayushman Bharat Digital Mission: An analytical cross-sectional study among outpatient department attendees. *BMC Health Services Research*, 26, Article 512. <https://doi.org/10.1186/s12913-026-14314-7>

²⁸⁶ Software Freedom Law Center, India. (2024, February 9). *The BTS (Behind the Screens) of privacy policies: Health apps edition*. <https://sflc.in/the-bts-behind-the-screens-of-privacy-policies-health-apps-edition/>

²⁸⁷ National Health Authority. (2021). *Consultation paper on health data retention policy*. Government of India, Ministry of Health and Family Welfare. https://abdm.gov.in/strapicms/uploads/Consultation_Paper_on_Health_Data_Retention_Policy_21_28557f9a6a.pdf

²⁸⁸ National Health Authority. (2021). *Consultation paper on health data retention policy*. Government of India, Ministry of Health and Family Welfare. https://abdm.gov.in/strapicms/uploads/Consultation_Paper_on_Health_Data_Retention_Policy_21_28557f9a6a.pdf

²⁸⁹ National Health Authority. (2024). *Health management policy*. Government of India, Ministry of Health and Family Welfare. https://abdm.gov.in/strapicms/uploads/health_management_policy_bac9429a79.pdf

for handling contingencies such as privacy breaches of the data collected from devices, loss of the device and loss of data collected from the device. ABHA creation via offline modes is largely handled by ASHA workers, ANMs and other frontline workers, who have limited digital literacy and high workloads. The guidelines impose uniform obligations on participating entities and authorised personnel without accounting for varied capacities and only prescribe training requirements without clear specifications of minimum training standards, certifications and monitoring of such training for the safe collection, migration and disposal of personal data and for obtaining meaningful consent.

There are also critical gaps in regulatory oversight for privacy protection. While the mission blueprint recommends establishing a Privacy Operation Centre to drive compliance with privacy requirements, there is no clear public evidence of implementation. Moreover, there are no details on the structure and precise obligations of such a centre nor an articulation of threat models that could provide the requisite rationale for regulatory measures.²⁹⁰

4.5.2 User Control and Rights

The ABDM's architecture emphasises patient control of their health data. The health ID enables citizens to choose from various registration and verification methods and establishes procedures for deactivation and opting out from the ecosystem.²⁹¹ The ABDM-enabled PHR apps enable citizens to view, download and delete records linked to their health ID. However, certain profile details, such as name, gender and date of birth, cannot be edited in KYC-verified profiles but can be modified in self-declared profiles.²⁹²

In practice, user control is centred on consent management for sharing health data and the ability to access and manage linked records from patient-facing applications. Despite the centrality of consent, in the early stages of the mission, patient autonomy was undermined in instances where health IDs were issued to individuals without consent, and the pressure of scaling ABHA resulted in coercion at certain facilities.^{293,294}

4.5.3 Cybersecurity

The federated architecture of the ABDM can reduce concentration risk, i.e., the potential of large amounts of sensitive health data being compromised with a single successful breach. At the same time, however, the heterogeneous nature of the healthcare system, consisting of small- and mid-sized as well as large facilities with varying capacities for enforcing cybersecurity measures, makes systemic risk dependent on the weakest link.

²⁹⁰ Agrawal, P., Sharma, S., Sagar, A., & Banerjee, S. (2023). On health data architecture design. In S. Parsheera (Ed.), *Private and controversial: When public health and privacy meet in India*. HarperCollins India.

²⁹¹ National Health Authority. (n.d.). *Health ID*. Ayushman Bharat Digital Mission. https://abdm.gov.in/strapiCMS/uploads/Health_ID_f945603dd1.pdf

²⁹² National Health Authority. (n.d.). *ABHA mobile app FAQ*. Ayushman Bharat Digital Mission. <https://abdm.gov.in/faq/abhamobileapp>

²⁹³ Chandrasekhar, R. (2024). Datafication, power, and publics in India's national digital health ecosystem. *Socio-Legal Review*, 20(1), 1-38. <https://repository.nls.ac.in/slr/vol20/iss1/1/>

²⁹⁴ Radhakrishnan, R. (2021, November 8). *Health data as wealth: Understanding patient rights in India within a digital ecosystem through a feminist approach*. Internet Democracy Project. <https://internetdemocracy.in/reports/health-data-as-wealth/>

The National Digital Health Blueprint recommended establishing a dedicated Health-Cloud (H-Cloud) with stronger security and privacy policies for deploying identities and registries as well as a Security Operations Centre.²⁹⁵ The NHA currently hosts the ABDM building blocks on private cloud infrastructure and only recently rolled out plans for a managed Security Operations Centre for “round-the-clock monitoring, threat detection, incident response, and compliance management.”²⁹⁶

Technology solutions integrating with ABDM must undergo a Web Application Security Audit (WASA) to assess vulnerabilities and verify adherence to security standards prescribed in the HDMP.²⁹⁷ These include adherence to encryption standards prescribed by the ABDM to ensure secure transmission of patient data.²⁹⁸ These audits are conducted by agencies empanelled by CERT-In.²⁹⁹ The NHA has also specified encryption standards for personal data at rest and in transit under the guidelines for the offline creation of ABHA using digital devices.³⁰⁰ Smaller clinics and standalone healthcare facilities have limited capabilities to implement robust cybersecurity and compliance measures. In practice, many facilities using ABDM-enabled HMIS solutions may lack dedicated technical capacity for maintaining advanced security safeguards, creating a gap between policy-level security requirements and ground-level operational readiness.

4.6 Recommendations

Overall, the mission has made significant progress in expanding coverage and generating incremental impact. However, sustaining this momentum would require a greater shift towards approaches focused on delivering meaningful outcomes. This can be achieved by building on the value proposition of the ABDM through prioritising a few high-impact use cases from the demand and supply side of healthcare,³⁰¹ streamlining the structure and disbursement of financial incentives, centring broader inclusivity in the design of infrastructure and applications, strengthening stakeholder capacity for engagement and ensuring trustworthiness through robust privacy-enhancing techniques and cybersecurity frameworks. Drawing on stakeholder insights, we propose the following recommendations.

Build on the value proposition of ABDM components: A success metric for the mission, in addition to onboarding professionals and facilities onto ABDM registries, would be the active utilisation of these components. For instance, linking the health professional identity and

²⁹⁵ Ministry of Health and Family Welfare. (2019). *Final report on National Digital Health Blueprint (NDHB)*. Government of India. https://mohfw.gov.in/sites/default/files/Final%20NDHB%20report_0.pdf

²⁹⁶ Telecommunications Consultants India Limited. (n.d.). *Tender document*. https://www.tcil.net.in/tender/pdf/25f2537_1.pdf

²⁹⁷ National Health Authority. (n.d.). *Sandbox exit*. Ayushman Bharat Digital Mission Sandbox Documentation. <https://sandbox.abdm.gov.in/sandbox/v3/new-documentation?doc=SandboxExit>

²⁹⁸ Open Healthcare Network. (n.d.). *ABDM*. OHC Docs. <https://docs.ohc.network/docs/care/ABDM/>

²⁹⁹ Choudhary, J. (2026, March 18). *ABDM certification process explained: Complete guide from sandbox to production (2026)*. *Nirmitee*. <https://nirmitee.io/blog/abdm-certification-process-sandbox-to-production-guide/>

³⁰⁰ National Health Authority. (2022, January). *Guidelines for offline ABHA generation using digital devices*. Government of India, Ministry of Health and Family Welfare. https://abdm.gov.in/strapicms/uploads/Guidelines_Offline_ABHA_generation_using_digital_devices_023a71b9cc.pdf

³⁰¹ Roundtable stakeholder insights.

registry to registrations, licence renewals and no-objection certifications, as planned under Unified Digital Services,³⁰² can create efficiencies for healthcare professionals, provided parallel offline process requirements (leading to duplication of efforts) are eliminated. Moreover, promoting solutions that seamlessly embed ABDM into routine clinical workflows through simplified interfaces and automation that reduce the “click tax” for clinicians and catalyse adoption.³⁰³ This is in addition to building potentially high-impact use cases for emergency care, chronic disease management and surgical pathways.

Restructure financial incentives and harmonise regulations: Feedback and lessons learned from the financial incentive scheme need to be considered. Some health tech companies and startups have reported delays in payment clearances, confusion on amounts due and difficulties tracking frequent changes from new rules notified every six months, all of which can create disillusionment among ecosystem partners. These issues need to be streamlined. An extended window of approximately 12-24 months must be provided for each notification. Performance-linked incentives can also be considered for frontline workers at the community level, such as Accredited Social Health Activists (ASHAs) and Auxiliary Nurse Midwife (ANMs), to accelerate adoption.³⁰⁴ Moreover, vendors of health tech solutions face complex regulations, sometimes with conflicting mandates, which can create compliance anxiety and stifle innovation. The ABDM should therefore support regulatory convergence by setting a uniform digital health regulatory standard aligned with the requirements of various regulatory authorities.

Improve reporting of outcome-focused metrics: To enhance transparency and accountability, there is a need to strengthen the monitoring and evaluation framework through shifting the focus of key performance indicators (KPIs) from inputs to outcomes.³⁰⁵ Through systematic collation of data from states, dashboards could incorporate measurable average efficiency gains for patients, healthcare providers, insurance companies, administrators and others in the ecosystem. Account aggregator ecosystem³⁰⁶ statistics could be drawn upon to include meaningful usage measures such as the number of consent requests sent and fulfilled, the amount of data exchanged and appropriate grievance redressal metrics such as resolution speed and first response time.

Strengthen inclusivity in design: This could take the form of targeted awareness strategy and technical support sessions, particularly for socioeconomically weaker sections. Similar to the

³⁰² National Health Authority. (n.d.). *Healthcare Professionals Registry (HPR)*. Government of India, Ayushman Bharat Digital Mission. <https://hspbx.abdm.gov.in/nhpr/v4/home>

³⁰³ Das, B., & Khan, M. (2026, April). *Economics of DPI in healthcare: Catalysing digital health innovation through ABDM* (Policy Brief No. 11). Indian Council for Research on International Economic Relations (ICRIER). <https://icrier.org/pdf/Economics-of-DPI-inHealthcare.pdf>

³⁰⁴ Das, B., & Khan, M. (2026, April). *Economics of DPI in healthcare: Catalysing digital health innovation through ABDM* (Policy Brief No. 11). Indian Council for Research on International Economic Relations (ICRIER). <https://icrier.org/pdf/Economics-of-DPI-inHealthcare.pdf>

³⁰⁵ Kadambi, P., Joseph, P. T., & Ajitsaria, D. (2025). *Ayushman Bharat Digital Mission: From infrastructure to impact—A tri-lens assessment of India's digital health system*. Figshare. <https://doi.org/10.6084/m9.figshare.30971167>

³⁰⁶ Sahamati. (n.d.). *Account aggregator ecosystem dashboard*. <https://sahamati.org.in/aa-dashboard/>

microsite project, a collaborative effort among public officials, technology entrepreneurs and digital health research institutions could help develop a broad equity framework³⁰⁷ and assessment tools for inclusive ABDM-compliant digital health solutions. To ensure buy-in from the supply side of healthcare, ABDM-integrated applications must be co-created with clinicians and frontline workers, and regulatory bodies such as the National Medical Commission should be engaged to ensure the relevance and usability of solutions. These applications should also undergo rigorous scientific evaluations for scalability and replicability. Additionally, the NHA could consider mandating periodic accessibility and usability audits for ABDM-compliant applications, including compliance with multilingual support and accessibility standards for persons with disabilities. Regional language interfaces and low-literacy-friendly workflows in PHR applications may also be incorporated as part of ABDM certification requirements. Additionally, establishing patient and community advisory mechanisms at the national or state levels could help incorporate user feedback from diverse demographic groups into ongoing design and implementation decisions. At the grassroots level, frontline health workers such as Community Health Officers (CHOs) and ASHA workers struggle with fragmented public health portals and require strengthened training on linking ABDM with existing applications such as e-Sanjeevani.

Capacity building and cybersecurity: Digital health capacity-building needs to be institutionalised at the state level through methods such as integration with medical/nursing curricula, continuous learning through periodic refresher modules and incentivisation through the certification of digital competencies.³⁰⁸ To address ambiguities surrounding data governance, there is a need for clearer articulation of the alignment between the ABDM and the DPDP Act through comprehensive documentation that clarifies liability ownership, provides scenario-based examples for data breaches and identifies the authorities responsible for guidance, review and compliance certification.^{309,310} Other important steps for strengthening privacy and security could include stringent penalties for data breaches to deter negligence, establishing and incentivising participation in a data protection certification program for providers in the sector and creating cybersecurity best practices tailored to healthcare that are focused on advanced encryption technologies, secure data transfer protocols and multi-factor authentication systems.³¹¹

Secondary use framework for ABDM data: Given the growing scale of longitudinal digital health data within the ABDM ecosystem, there is a need for a clearly defined governance framework for the secondary use of health data for research, innovation, public health

³⁰⁷ Country Connector on Private Sector in Health. (2022, June 2). *Mutual learning on digital health ecosystems*.

<https://ccpsh.org/blog/mutual-learning-digital-health-ecosystems>

³⁰⁸ International Innovation Corps & UP-TSU. (2025). *Digital health capacity building blueprint*.

https://static1.squarespace.com/static/57ec07bb46c3c4749838974b/t/691418527bafc50f089e0dae/1762924626218/DHCB+Blueprint_Nov2025.pdf

³⁰⁹ Stakeholder insights.

³¹⁰ Das, B., & Khan, M. (2026, April). *Economics of DPI in healthcare: Catalysing digital health innovation through ABDM* (Policy Brief No. 11). Indian Council for Research on International Economic Relations (ICRIER). <https://icrier.org/pdf/Economics-of-DPI-inHealthcare.pdf>

³¹¹ Garg, O., Choksi, M., & Mokashi, T. (2025). *Strengthening health governance and data protection through the Digital Data Protection Act, 2023 in India's digital health ecosystem* [Poster]. PMAC 2025. <https://pmac-2025.com/uploads/poster/A089-OSHIARG-6635.pdf>

planning and policymaking. Such a framework should establish standardised protocols for the de-identification and anonymisation of datasets, define permissible use cases and incorporate independent ethical oversight mechanisms for data access and usage approvals. It should also outline accountability measures, audit trails and benefit-sharing principles to ensure that public value generated from ABDM-linked data contributes equitably to health system strengthening while safeguarding individual privacy and preventing misuse or commercial exploitation of sensitive health information.

4.7 Comparative Analysis: DPI-Enabled Healthcare Provisioning in India and Australia

India and Australia have pursued distinct models of digital health transformation, shaped by their respective objectives, healthcare contexts and levels of digital maturity. Despite these differences, the ABDM and My Health Record share a common vision of improving healthcare delivery through the efficient exchange of health information to support patient-centred care. Table 9 provides a comparison of the two systems across key dimensions drawn from the evaluative framework and is followed by a discussion of the strengths and limitations associated with their respective design and implementation choices.

Table 9: Comparing India’s and Australia’s DPI Architectures for Healthcare Provisioning

Dimension	My Health Record — Australia (MHR)	Ayushman Bharat Digital Mission — India (ABDM)
A. DPI TECHNICAL ARCHITECTURE		
DPI Architecture Model	Centralised repository model. A national clinical data repository stores all health documents. Central governance by Australian Digital Health Agency (ADHA) as system operator.	Federated architecture. Health records stored at/near the point of care, not in a central store. Infrastructure managed by the National Health Authority (NHA).
Digital Identity Layer	Healthcare Identifiers (HI) Service: Unique IDs for individuals (IHI), providers (HPI-I) and organisations (HPI-O). NASH PKI: Certificates for authentication, ³¹² digital signing and encryption.	Ayushman Bharat Health Account (ABHA): 14-digit unique health ID + alphanumeric ABHA address. Healthcare Professionals Registry (HPR) and Healthcare Facility Registry (HFR) for provider/facility identity.
Data Exchange Layer	B2B APIs and Fast Healthcare Interoperability Resources (FHIR) gateway. ³¹³ Integration with 110+ software products. Conformance-based connection; providers must satisfy security and technical standards before connecting.	Health Information Exchange–Consent Manager (HIE-CM) as data gateway, National Health Claims Exchange (NHCX) as insurance claims processing gateway, Unified Health Interface (UHI) for service discovery.

³¹² National Authentication Service for Health (NASH) PKI (Public Key Infrastructure). NASH PKI is Australia’s national digital certificate system specifically built for the healthcare sector.

³¹³ FHIR (Fast Healthcare Interoperability Resources) is a standard for exchanging healthcare information electronically. It is adopted worldwide for the healthcare sector.

Interoperability Standard	FHIR gateway/API environment; structured document types; conformance profiles enforced for all connecting systems.	FHIR R4 recommended, but PDF uploads permitted in early stages. Semantic interoperability not yet widespread.
B. PILLAR 1 — ACCESSIBILITY & INCLUSIVITY		
Participation Model	Opt-out since 2019: Australians are automatically registered; can cancel at any time. Prior to 2019: opt-in model with low uptake (<10% active use despite 80% GP registration).	Opt-in model but increasingly being embedded in hospital workflows and mandated for linkage with healthcare services.
Inclusion for Underserved Groups	Telephone support and assisted identity verification available. No specific offline ABHA-equivalent. Disparities remain for remote/rural, low-digital-literacy and low-income populations.	Offline ABHA generation (paper-based and digital devices) addresses identity layer for low-connectivity users but not transaction barriers. ABDM portal complies with accessibility standards. ³¹⁴ Gender parity in ABHA generation, but active use by women is lower.
Digital Literacy / Onboarding Friction	~25% of potential users fail to complete the myGov-to-MHR linking workflow, which is the most commonly reported onboarding barrier.	Awareness, lack of perceived benefit and capacity to navigate digital workflows remain major barriers. Device/data-cost constraints for economically weaker groups.
Feedback & Grievance	Office of the Australian Information Commissioner (OAIC) investigates privacy complaints; 30-day response target. Helpline and online support available. Limited outreach to marginalised groups.	Multi-channel grievance portal (web, toll-free call centre in six languages, postal). 30-day TAT prescribed but actual metrics not publicly reported. Multilingual AI-based support being developed.
C. PILLAR 2 — EFFICIENCY		
Process Efficiency Gains	Consumer use ↑47.6%; provider cross-organisational viewing ↑67% (2024-25). Sharing by default policy: Mandatory upload of pathology and imaging reports, improving timeliness. myGov login step removed for returning users.	Scan and Share: 219.56 million tokens issued; OPD registration time reduced from 70 minutes to 47 minutes (Bihar). ³¹⁵ Clinical Decision Support System (CDSS) integration reduced consultation time from 5-7 minutes to 3-4 minutes (Karnataka). ³¹⁶
Cost Efficiency	Free to consumers. Indirect savings: Reduced duplicate testing, better care coordination, fewer medication errors. No publicly reported cost-per-transaction or government efficiency metrics.	Free to consumers. Digital Health Incentive Scheme (DHIS) subsidises adoption for facilities and health tech companies. NHCX aims to reduce claims processing cost and delays. Quantified system-wide cost savings not yet reported; however, similar indirect savings likely.
Onboarding / Integration Efficiency	Registration, conformance, and connection processes described as “lengthy”. Western and South Australia	Sandbox environment for developer testing. API version changes without adequate deprecation windows created rework burden for smaller

³¹⁴ World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 level AA ensure accessibility of the portal for visually impaired individuals through assistive technologies such as screen readers. Ayushman Bharat Digital Mission. (n.d.). *Screen reader access*. Government of India. <https://abdm.gov.in/screen-reader-access>

³¹⁵ National Health Authority. (2026, March 24). *Bihar and Rajasthan: Digital health best practices | StateXchange* [Video]. YouTube. <https://www.youtube.com/watch?v=bkKgfZiZjE>

³¹⁶ National Health Authority. (2025, September 11). *Digital health innovations in India | State success stories | #ABDM webinar* [Video]. YouTube. https://www.youtube.com/watch?v=mywo4_BfXys

	Health structured pathology uploads delayed to 2025-26.	vendors. Some registry onboarding delays reported.
System Capacity & Scalability	2 billion+ documents uploaded; scalable across remote communities. Clinical incidents rare at 1.5 per million interactions. Limited public reporting on outage/downtime metrics.	833 million+ ABHAs; 1.135 billion+ health records linked. Scalability dependent on state digital maturity. Limited disclosure of uptime or disaster recovery metrics.
Innovation	FHIR-based interoperability; 110+ integrated software products; expansion into aged care and multidisciplinary care coordination.	Health-tech startups building ABDM “connector” APIs (cutting onboarding cost by 50%+). Use of AI and ABDM components for fraud detection and management in the insurance industry, personalised healthcare recommendations, etc.
D. PILLAR 3 — SECURITY		
Legal Framework	My Health Records Act 2012 (primary legislation, with criminal/civil penalties). Privacy Act 1988. Healthcare Identifiers Act 2010. My Health Records Rule 2016 and Regulation 2026.	No overarching primary legislation for digital health. Governed by Health Data Management Policy 2020 (executive policy, non-justiciable) and Digital Personal Data Protection Act (DPDPA) 2023. Proposed DISHA legislation abandoned.
Privacy Architecture	Privacy-by-design: Purpose limitation, role-based access, encryption (ASD-compliant). ³¹⁷ Consumer controls: Record Access Code (RAC), ³¹⁸ Limited Document Access Code (LDAC), ³¹⁹ access history, deletion rights. Opt-out consent model: Routine provider access does not require per-transaction consent.	Privacy-by-design: Data minimisation (ABHA and registries require minimal attributes), consent artefact with granular dimensions (purpose, HI type, requester, range, validity). Consent-based architecture for data sharing. DPDPA permits processing without explicit consent for public health functions.
Data Storage & Sovereignty	Centralised domestic storage. Governed by ADHA as System Operator under Protective Security Policy Framework (PSPF). ³²⁰ High-grade encryption; ISM ‘Protected’ certification. ³²¹	Federated storage at or near point of care. NHA hosts ABDM building blocks on private cloud. Security Operations Centre recently rolled out.
Cybersecurity Governance	Dedicated CISO. Two specialist teams: Cyber Operations (monitoring, threat intelligence, incident response) and Cyber Solutions (architecture, assurance, compliance). ISM ‘Protected’ certification;	CISO and Data Protection Officer responsible for periodic review. Web Application Security Audits (WASA) and annual Vulnerability Assessment and Penetration Testing (VAPT) required for all connecting solutions; audited by CERT-IN

³¹⁷ ASD stands for the Australian Signals Directorate – Australia’s national cybersecurity authority. ASD-compliant encryption specifically means encryption that follows the ASD’s Information Security Manual (ISM) and its Guidelines for Cryptography.

³¹⁸ A Record Access Code (RAC) is a four to eight character code set by an individual allowing them to control which healthcare provider organisations have access to their My Health Record. If an individual sets a RAC, then visits a healthcare provider organisation that has not previously accessed their My Health Record, they will need to provide their RAC to the healthcare provider in order for them to access the record like a PIN.

³¹⁹ A Limited Document Access Code (LDAC) is an 8-20-character code set by an individual allowing them to control which healthcare provider organisations have access to specific clinical documents they have marked as ‘Restricted’.

³²⁰ The Protective Security Policy Framework (PSPF) sets out Australian Government policy across six security domains. It prescribes what Australian Government entities must do domestically and internationally to protect their people, information and resources.

³²¹ The Information Security Manual (ISM) provides detailed technical and governance controls that organisations can apply using their risk management framework to protect systems, applications and data from cyber threats. The Australian Government uses a tiered information security classification system. There are four levels of security classification: ‘Official: Sensitive,’ ‘Protected,’ ‘Secret’ and ‘Top Secret.’ To achieve ISM Protected certification, a system must undergo an IRAP assessment, conducted by an ASD-accredited independent assessor, who examines security controls, encryption, access management, physical data centres, incident response and risk management.

	IRAP assessments; ³²² penetration testing; pre-release testing.	empanelled agencies. Encryption standards for data at rest and in transit mandated.
Breach Response	Mandatory breach notification to ADHA and Information Commissioner “as soon as practicable.” 18 breach notifications in 2024-25, all closed. OAIC completed two digital health assessments in 2024-25.	HDMP requires notification to NHA and CERT-IN. Smaller facilities have limited capacity for robust cybersecurity, creating systemic risk at the weakest link.
User Control & Rights	Users can restrict access, restrict documents, remove documents, manage representatives, view full access history, set notifications. Can permanently delete entire record. Limited ability to edit provider-originated clinical data.	Users can view, download and delete linked records via PHR app. Consent artefact allows granular control over sharing. KYC-verified profiles cannot edit certain demographic attributes. Limited ability to edit provider-originated clinical data.
Regulatory Oversight	OAIC independently monitors privacy compliance, investigates complaints, and publishes annual digital health reports. Australian National Audit Office (ANAO) ³²³ has audited MHR implementation. Multi-layer independent oversight.	No dedicated digital health regulatory authority. DPDP Act enforcement through Data Protection Board (not yet fully operational). Privacy Operation Centre recommended in blueprint but there is limited publicly available evidence in practice.

Both ABDM and My Health Record began as opt-in systems but gradually incorporated mandates and opt-out mechanisms as voluntary participation alone proved insufficient to achieve scale. India’s choice of an open-API-based and federated technical architecture leverages existing systems for information exchange and offers the advantage of reducing duplication in data storage, minimising risks of a single point of failure and data aggregation and enabling diverse applications and use cases. However, it also places greater interoperability burden on providers and vendors, with the consequence that information may remain fragmented, with staggered adoption. While the centralised data storage model adopted by Australia’s My Health Record necessitates significant investments and ongoing maintenance with system scale-up and poses risks of misuse and large-scale breaches, it also reduces interoperability complexity after integration. A centralised architectural design also enables more feasible and relatively direct policy levers, such as mandatory upload requirements from lagging provider segments, to improve the completeness of records, vis-à-vis a federated design.

The ABDM’s decentralised governance model offers the flexibility to leverage a diverse ecosystem for innovation and scale and offers other key strengths such as shared implementation capacity and adaptability but also has limitations such as coordination complexity, incentive misalignment, dependence on the capacity of sub-national units and

³²² IRAP stands for the Infosec Registered Assessors Program (also written as Information Security Registered Assessors Program). The Australian Signals Directorate (ASD), via IRAP, provides organisations with access to cybersecurity professionals to conduct high-quality, independent security assessment services. An IRAP security assessment helps organisations understand their system’s security strengths and weaknesses and provides recommendations that can be utilised as part of their organisational security program.

³²³ ANAO is a specialist public-sector practice providing a range of audit and assurance services to the Parliament and Commonwealth entities. ANAO provides the highest level of independent accountability for MHR – parliamentary-level scrutiny that goes beyond internal governance or regulatory oversight. It is what allows Parliament and the Australian public to know whether public money spent on MHR is achieving its intended results and whether risks are being managed appropriately.

diffused accountability. The centralised governance of the My Health Record under a dedicated legislative framework ensures clearer accountability, uniform policy implementation and simplified stakeholder coordination and decision-making. At the same time, this risks top-down implementation that may not reflect the diverse operational realities of providers and reduces ecosystem dynamism.

The ABDM's privacy and security architecture offers stronger patient control over data exchange and reduced risks of concentration and data aggregation. However, this is accompanied by greater operational complexity, a larger attack surface and a distributed security burden among entities with varying cybersecurity maturity, which can affect overall system resilience. The stewardship of My Health Record under a single agency enables the consistent implementation of security controls across the system and is supported by a strong legislative framework. However, this comes with trade-offs, including less granular consent mechanisms and greater centralisation risks, with a systemic compromise potentially affecting a large volume of health information.

4.8 Conclusion

An analysis of India's ABDM and Australia's My Health Record indicates that the development of robust interoperable digital health architectures, governance and policy structures for facilitating safe use, effective models of private-sector engagement for scale-up and innovation, and cyber risk management frameworks are critical for achieving potential gains from digital health transformation.

While both systems seek to enhance healthcare delivery, India's adoption of the DPI model through a federated architecture reflects a context-specific design choice well suited for its vast geography and population size. Early investments in foundational DPI elements such as national digital identity and payments provided the requisite enabling infrastructure for building and expanding sectoral technological components and high-impact use cases such as Scan and Share and Scan and Pay, which have delivered early improvements in patient experience. In the years since its inception, the mission has progressed through an iterative approach, through the gradual rollout of new components and functionalities following consultations, supported by a partner ecosystem of diverse stakeholders leveraging their expertise in technology, capacity building, research and monitoring to drive the mission's design and implementation. While significant strides continue to be made in the diffusion of the infrastructure, continued momentum would depend on securing buy-in from the entire healthcare ecosystem. This remains challenging due to misaligned incentives, coordination complexities and technical and governance issues. The path forward lies in enhancing systemic readiness for sustained uptake of the infrastructure across the country's heterogeneous healthcare landscape, strengthening value creation of the technological components for all stakeholders, reforming incentives and improving institutional coordination mechanisms to create a greater role for states beyond implementation in

shaping the mission, thereby promoting shared ownership and advancing meaningful cooperative federalism. Moreover, while the ABDM architecture fares well on the two core security design principles of data minimalism and structural decentralisation, which help safeguard sensitive records and limit the cascading effects of a breach, the third principle of consequence absorption needs strengthening. This means ensuring that individual digital systems in health facilities are prepared for fast containment and clear recovery paths and that the risks of cybersecurity attacks are absorbed by system operators rather than citizens.

Australia's choice of a centralised repository model in the design of My Health Record is appropriate for a relatively smaller population and health sector, which makes such investments feasible and simplifies provider integration. The system's opt-out model was instrumental in accelerating coverage of citizens in the initial years, which in turn catalysed broad-based adoption and active use among other entities. A strong legislative framework governing health data management, providing clear stakeholder roles and responsibilities and robust accountability measures, coupled with effective leadership and cybersecurity risk management processes, constitutes key complementary strengths of the system. However, consumer onboarding frictions and the need for implementation support to segments lagging in information-sharing are challenges that need to be addressed. Beyond My Health Record, Australia's experience in digital health projects provides key practices for engendering trust; a benevolent customer-centric approach; radical honesty with key stakeholders; and seeking feedback, rigorous development, validation and monitoring, preserving human decision-making discretion and aligning the authorising environment.

The analysis of the progress and gaps in both systems also highlights a common set of future priorities. Measurement and reporting should move beyond system utilisation to evaluate impacts on care delivery and the value accrued to various stakeholders, thereby informing a more outcome-oriented evolution of these systems. Additionally, both systems would benefit from simplifying their legal and regulatory frameworks to facilitate stakeholder understanding and compliance, alongside more transparent reporting of grievance redressal metrics to strengthen accountability and trust.

5. Key Lessons for DPI-Enabled Public Service Delivery

The two case studies presented in this report examine the application of the DPI approach across two distinct public service domains: welfare delivery and healthcare. While these sectors differ in their objectives, institutional arrangements and stakeholder ecosystems, they reveal a common set of lessons about how DPI can be designed and governed to improve public service delivery. Drawing on the comparative analysis of India and Australia, this chapter distils a set of cross-cutting design and implementation lessons, particularly for countries in the Asia-Pacific region that are considering adopting this paradigm to address critical challenges in their own contexts.

The choice of DPI architecture should reflect local contexts, technical feasibility and embed inclusivity in design.

The assessment highlights key technical architectural choices that policymakers face when designing DPI, such as centralised versus decentralised models and their respective trade-offs. These choices should be guided by a clear articulation of the objectives and value proposition of introducing DPI for a particular public service while accounting for the ecosystem, features of the deployment landscape and state capacity. Together, these factors help determine the feasibility of different architectural approaches. To unlock the full potential of the DPI paradigm in enhancing the user experience of public service delivery, technical design must prioritise seamless onboarding, inclusive interfaces and capacity building for last-mile functionaries. To the extent possible, it should also incorporate a participatory design process that reveals the diverse challenges faced by different demographic groups in navigating digital systems, helping ensure that systems are designed for the weakest link.

DPI governance should be backed by supportive legislative mandate, sound institutional frameworks and effective grievance redressal mechanisms to strengthen accountability and public trust.

A dedicated legislative framework underpinning DPI implementation is essential for establishing statutory oversight and accountability mechanisms, which in turn can enable more effective implementation of safeguards and strengthen public confidence in systems. Institutional structures must be well-defined, with clear delineation of roles and responsibilities, adequate financing, sustained capacity building, as well as effective coordination mechanisms and incentive design to align diverse stakeholder interests towards common goals. The adoption and sustained use of DPI can also be strengthened through responsive grievance redressal processes that enable users to lodge complaints easily and ensure their timely resolution. This can be achieved by simplifying workflows that minimise citizens' need to engage with multiple agencies, providing transparent mechanisms for tracking complaints and systematically incorporating user feedback into service improvements. Together, these measures enhance accountability, responsiveness and public trust in DPI-enabled public service. An important aspect of governance is also ensuring that DPI implementation is accompanied by internal public sector data capability, with sustained capacity building for civil servants in data literacy, privacy and audit analytics.

Security and privacy should be embedded into DPI by design rather than treated as an afterthought.

As DPI systems become increasingly interoperable and data-intensive, security and privacy should be integrated into DPI design from the outset rather than added as retrospective safeguards. Embedding privacy-by-design measures such as data minimisation, purpose

limitation, secure-by-default system architecture, consent management, tokenisation and robust API governance, complemented by privacy impact assessments, can strengthen trust while reducing vulnerabilities across the ecosystem. At the same time, security should extend beyond protecting core infrastructure to encompass the entire service delivery chain, including implementing agencies, intermediaries, third-party providers and end-user interfaces. Such an approach not only reduces risks but also ensures resilient, trustworthy and long-term sustainability of DPI-enabled public services.

Move beyond breach prevention by building operational resilience into DPI governance.

DPI should be assessed not only by the security incidents it prevents but also by its ability to contain harm, maintain essential services and restore affected users quickly when incidents occur. As cyber threats evolve, past security performance alone is not a reliable indicator of future readiness. Governments should adopt resilience standards requiring scenario-based stress testing, monitoring and learning; continuity arrangements for essential services; defined detection and recovery timelines; and clear institutional responsibility for remediation. These standards should embed data minimisation, structural decentralisation and consequence absorption: collect only what is necessary; avoid concentrations of data and control that create catastrophic single points of failure; and ensure that the costs of fraud, data exposure or service disruption are borne by responsible institutions rather than citizens. The shared security agenda for countries building DPI should focus on measuring systems against these standards, measuring what truly matters (such as harms absorbed and recovery time) and trading evidence on successes and failures across national stacks.

Foundational DPI should be complemented by sector-specific institutions and governance.

Foundational DPI components such as digital identity, payments and data exchange create a common, sector-agnostic digital infrastructure that can accelerate the delivery of a broad range of public services. While foundational DPI can reduce the cost and complexity of digital transformation, sustained adoption and impact depend on building complementary sector-specific ecosystems that enable diverse stakeholders to participate, innovate and deliver services effectively.

Digital public services must remain human-centred despite increasing digitalisation.

Both case studies demonstrate that digital technologies complement rather than replace human institutions in public service delivery. Despite increasing automation and interoperability, effective implementation continues to depend on frontline workers, service providers, implementation partners and accessible physical service channels that help citizens navigate digital systems. Human support remains particularly important for vulnerable populations, as well as for grievance resolution and for building confidence in new digital services. As governments expand their use of DPI, investments in institutional capacity, digital

literacy and last-mile support should evolve alongside technological infrastructure to ensure that digital transformation remains inclusive and trusted.

Performance monitoring of DPI should prioritise public value and iterative learning.

Both the welfare delivery (DBT) and healthcare (ABDM) case studies demonstrate that DPI requires substantial investments throughout its lifecycle, from conceptualisation and development to implementation and ecosystem activation. As such investments are largely financed through public funds, policymakers must continually evaluate and build on the public value delivered by the infrastructure. Performance monitoring and reporting must move beyond measuring outputs and administrative efficiency gains to prioritise user experience and public outcomes. The evolution of DPI should be informed by such metrics, and alternative approaches to its design and implementation can also be experimented with for iterative learning and adaptation.

The lessons emerging from both case studies underscore that the success of DPI-enabled public service delivery depends not only on the deployment of interoperable digital infrastructure but equally on the institutional, governance and implementation ecosystems that support it. As countries increasingly adopt DPI across sectors, the focus should extend beyond technological deployment towards building systems that are responsive, inclusive, secure and capable of adapting to evolving user needs and policy priorities. Rather than prescribing a single model for implementation, the lessons presented in this report offer broad considerations to guide policymakers in designing DPI-enabled public services suited to their own institutional, administrative and societal contexts.

Annexure 1: DPI for Public Service Delivery Assessment Framework

Pillar	Factor	Element	What to Assess (indicative and non-exhaustive)
Accessibility and Inclusivity	User Diversity and Reach	Gender Inclusion	What proportion of female beneficiaries are served by DPI-based public service delivery systems? Are there tailored outreach or support measures for women (e.g., gender-sensitive interfaces, women-led digital literacy sessions)? What are the barriers and enablers for women's registration and regular use?
		Disability Access	Are interfaces accessible (screen readers, audio prompts, tactile/Braille options)? Are physical helpdesks/kiosks equipped for people with disabilities? Are alternative authentication modes (e.g., OTP, PIN, assisted biometrics) available?
		Inclusion of Migrants and Mobile Populations	Are DPI-linked benefits and identity credentials portable across states and administrative boundaries, or are entitlements tied to the state or district of original registration? Do internal migrants face barriers to accessing DPI-enabled services outside their registered home state? If yes, what mechanisms exist to address this? Are there pathways for migrants to update their registered address or location without losing existing entitlements or triggering re-enrolment requirements? Are alternative enrolment or identity verification pathways available for individuals without stable addresses, including homeless persons and seasonal workers? Is there data on the proportion of migrant or mobile workers excluded from DPI-linked schemes due to residency-based registration requirements?
		Socioeconomic and Literacy Inclusion	What share of users are from low-income/low-literacy backgrounds? Are services in vernacular languages? Is assisted registration/support provided for illiterate users? Is affordability (device/data costs) a barrier, and if so, how is it addressed?
	Access Mechanism	Geographic Coverage	What percentage of users (and service points) are in rural, remote, tribal or marginalised regions? What disparities exist in registration, service usage or benefit receipt by geography? What percentage of DBT/healthcare transactions occur in non-metro areas?
		Digital and Assisted Channels	Are both digital (online self-service) and assisted (offline, kiosk, phone) modes available for application, grievance and redressal? Is offline access (e.g., SMS, QR code, USSD) supported for areas with poor internet connectivity?
		Inclusion Efforts to Engage Minority/Marginalised Groups	Do systems monitor and report on beneficiary demographics (by caste, religion, race, disability, region)? What mechanisms exist to proactively include marginalised populations and track exclusion errors? Are there anti-discrimination safeguards or culturally sensitive features? Are there mechanisms to proactively identify and support marginalised individuals excluded from services due to, <i>inter alia</i> , authentication failure, documentation barriers or physical inaccessibility? Do DPI schemes include specific provisions, such as proxy authentication or caregiver-assisted access, to ensure continuity of benefits for beneficiaries who cannot comply with standard digital authentication requirements due to age, disability, health and/or mobility concerns?
	Feedback and Redressal	Grievance Redressal Channels	Are there accessible (multi-channel, multi-language) complaint and help desk mechanisms? What is the average turnaround time for resolving access-related grievances? Are turnaround times for grievance resolution clearly defined and publicly disclosed? Is data on complaint types, volumes, actual resolution times

			and escalation rates systematically collected, published and used to improve service delivery? Are user feedback loops operational, especially for marginalised populations?
		Digital and Financial Literacy Support	What digital and financial literacy programmes are in place for first-time or low-literacy users, with targeted attention to women, elderly persons and marginalised groups? Are digital support agents, community resource people or assisted service points available in person and geographically accessible to underserved populations available in person? Are literacy programmes delivered in local and vernacular languages, with formats adapted for low-literacy users (e.g., audio, visual demonstration, peer-to-peer learning)? Is there evidence that literacy support translates into active and independent use of DPI services, rather than continued dependence on intermediaries for routine transactions? Are literacy programmes monitored and evaluated for reach and effectiveness, and regularly updated to reflect changes in DPI interfaces and processes?

Pillar	Factor	Element	What to Assess (indicative and non-exhaustive)
Efficiency	Optimising the Process	Improving/Simplifying the Process	Has there been any reduction in bureaucratic steps (e.g., through automated verification)? Have efficiency gains translated into improved service quality from citizen perspectives rather than solely administrative performance metrics? Can users self-serve end-to-end?
		Improvements in Time and Speed	What has been the difference in the time and speed of benefit transfer/receipt of service(s) before and after DPI implementation? Are there delays at particular stages (identity, verification, disbursement)? If yes, how are they remedied? Is there any data on the time saved by frontline workers?
	Cost Efficiency	For the system	What is the cost per service transaction for government, users and intermediaries (if any)? Have there been any savings on staff hours, fraud reduction/prevention, and/or resource use?
		For users	Has there been any reduction in travel/documentation costs? Is there any data? Are there any fees for services (if any)?
	System Capacity	Scalability and Resilience	How does the system handle increased loads (e.g., COVID-19 crisis cash transfers)? What platform downtimes/outages have occurred, and how were they managed?
	Innovation	Interoperability and Integration	Are identity, payment and data platforms interoperable across implementation agencies and third parties (if any)? Any examples of successful integrations with third-party or state schemes?
		Multiple Use Cases	Can the same DPI systems be used for several schemes/programs? If yes, are there any examples? Have DPI systems generated documented beneficial outcomes beyond their primary use case, such as increased financial activity among previously unbanked users, improved availability of administrative data for policy planning or private-sector innovation built on public DPI infrastructure? How are these spillover effects identified, measured and attributed?
		Innovation & Public-Private Partnerships	Has the use of DPIs led to the development of new products/services by the private sector? Are there any active collaborations between the government and the private sector?

Pillar	Factor	Element	What to Assess (indicative and non-exhaustive)
Security	Privacy and Data Protection	Privacy by Design	Are privacy-by-design principles (data minimisation, explicit user consent, purpose limitation) reflected in policy and technical architecture? Are consent processes clear and granular for users? Are data retention and deletion standards defined and monitored?
		Data Storage and Processing	Where is data stored (national/local/international)? Who controls it? Are regular audits performed? For vendors, are data-handling norms enforced contractually and technically? Are clear standards and audit mechanisms in place for partner or third-party access to data? Has there been evidence or risk of data misuse by non-state actors? Is access to data, applications and systems tightly controlled and monitored?
		User Control and Rights	Can users view, download, update or delete their own data? Are such procedures and processes clearly communicated and accessible?
	Cybersecurity	Governance	Is there a designated leader or team responsible for overseeing the cybersecurity in DPI? Have security risks for data, applications and systems been identified, regularly updated, communicated to stakeholders and embedded into the organisational risk framework? Are security risks formally accepted before systems go live and continuously reassessed during their operation? Are there periodic security audits?
		Identify	Is the business criticality of systems (cyber supply chains, infrastructure, operating system, applications and data) clearly defined and documented? Are the confidentiality, integrity and availability requirements for systems (cyber supply chains, infrastructure, operating systems, applications and data) determined and documented? Are security risks for systems (cyber supply chains, infrastructure, operating system, applications and data) identified and recorded? Are system interdependencies identified and documented, including the potential security impact on dependent systems if one is compromised?
		Protect	Are systems (infrastructure, operating systems and applications) securely planned, designed, deployed, maintained and decommissioned in accordance with both business and security requirements? Are systems (infrastructure, operating systems and applications) planned, designed, developed, tested, deployed, maintained and decommissioned using secure by design and secure by default principles and practices? Are vulnerabilities in systems (cyber supply chains, infrastructure, operating systems, applications and data) identified and mitigated in a timely manner? Is access to systems data (cyber supply chains, infrastructure, operating systems, applications and data) tightly controlled and monitored? Are data protection (encrypt data at rest and in transit) and backup measures effectively implemented? Is data communicated between different security domains controlled and inspectable? Are personnel trained and accountable for cybersecurity practices?
		Detect	Are security-related event logs centrally gathered, securely stored and promptly analysed to detect potential cybersecurity incidents? Are changes to security-related configurations centrally logged, securely stored and promptly analysed to detect potential cybersecurity threats? Are cybersecurity events promptly analysed to identify potential security incidents? Are cybersecurity event detection capabilities regularly evaluated for effectiveness and continuously refined?

		Respond	Are cybersecurity incidents reported quickly to all relevant internal and external stakeholders? Are cybersecurity incidents promptly analysed, contained, resolved and recovered from? Do response and recovery plans ensure business operations can continue during and after incidents? Are lessons learned from cybersecurity incidents documented, with improvement areas identified and addressed promptly?
		Recover	Are systems verified through assurance activities following a cybersecurity incident to confirm they are secure and capable of supporting the resumption of normal business operations? Are residual security risks, including inherited and shared risks, formally accepted prior to the resumption of normal business operations following a cybersecurity incident?
	Fraud and Risk Management	Authentication and Verification	Which authentication methods (biometrics, OTPs, two-factor, alternatives for users with disabilities or degraded biometrics) are in use? Do you collect data on the authentication and API error and failure rates, disaggregated by user group, geography and authentication method? Are these rates monitored proactively to identify systemic exclusion patterns requiring design or policy intervention? What de-duplication processes are in place to ensure unique registration?
		Fraud Monitoring and Response	Are there any processes for fraud/malpractice detection, notification and resolution? Are there processes for the detection of unauthorised access? How are they managed?
		Grievance Mechanisms for Security Breaches	Are beneficiaries/users informed and supported in case of personal data breaches or fraud? What recourse exists? Are clearly defined and accessible recourse pathways, such as helplines, in-person support and formal complaints mechanisms available to users affected by data breaches, identity fraud or unauthorised use of their personal data, with defined response timelines and escalation procedures? Is support provided to affected users, such as identity restoration assistance, benefit reinstatement where relevant and legal recourse guidance? Is this support accessible and regularly reviewed for effectiveness?
	Governance and Compliance	Legal and Regulatory Compliance	Compliance with laws (e.g., Personal Data Protection Bill, RBI/health sector norms)? Is there monitoring of third-party compliance where data is shared?
		Transparency and Accountability	Are there regular transparency reports, audit disclosures and independent reviews? Are there clear lines of accountability for data stewardship and incident management?
		User Trust and Communication	Are users regularly informed about system changes, privacy policies and breaches? How are user trust, perceptions of safety or reservations documented and addressed?
		Algorithmic Accountability	Transparency requirements for automated decision-making processes, such as disclosure of algorithmic logic and decision factors. User rights to explanation and contestation of algorithmic decisions. Mandatory fairness and bias audits for algorithms affecting service access or eligibility. Human review mechanisms for automated decisions, especially those with significant individual impact. Documentation requirements for algorithmic system development, training data and performance metrics.

Annexure 2: Direct Benefit Transfer Scheme in India

Table 2.1: Estimated Benefits/Gains from DBT and Other Governance Reforms

Ministry/ Department	Scheme Category	Estimated Savings/Benefits (in INR Crore)			Remarks
		Cumulative upto March 2023	April 2023 to March 2024	Cumulative upto March 2024	
Ministry of Petroleum and Natural Gas	PAHAL	73,443.34	403.15	73,846.49	Elimination of 4.23 crore duplicate, fake/non-existent, inactive LPG connections. In addition, number of non-subsidised LPG consumers is 2.38 crore . The aforesaid numbers (4.23 crore + 2.38 crore) include 1.15 crore “give-it-up” consumers.
Department of Food and Public Distribution	PDS	185,573.28	64,399.25	249,972.53	Deletion of 5.87 crore duplicate and fake/non-existent ration cards.
Department of Rural Development	MGNREGS	42,534.14	15,524.84	58,058.98	Deletion of 1.26 crore fake and duplicate job cards.
Department of Rural Development	NSAP	537.1	243.11	780.21	Deletion of 7.21 lakh duplicate, fake/non-existent, ineligible beneficiaries.
Ministry of Minority Affairs	SCHOLARSHIP SCHEME	1,916.79	380.024	2,296.81	Deletion of 37.77 lakh duplicate, fake/non-existent beneficiaries.
Department of Social Justice and Empowerment	SCHOLARSHIP SCHEME	1,054.65	0	1,054.65	Deletion of 12.28 lakh duplicate, fake/non-existent beneficiaries.
Ministry of Women and Child Development	OTHERS	1,523.75	0	1,523.75	Reduction of 98.8 lakh duplicate, fake/non-existent beneficiaries.
Department of Fertilizers	FERTILIZER	18,699.89	0	18,699.89	Reduction of 158.06 lakh metric tonnes of fertiliser sale to retailers.
Department of Agriculture and Farmers Welfare	PM-KISAN	22,106.14	0	22,106.14	Deletion of 2.1174 crore ineligible beneficiaries.
Ministry of Micro Small and Medium Enterprise	PMEGP	0	1,449.53	1,449.53	Deletion of 38,184 duplicate/ineligible beneficiaries.
OTHERS	OTHERS	1,175.58	173.49	1,349.07	
Total		348,564.66	82,573.39	431,138.05	

Table 2.2: Recorded incidents related to data leaks, security and Aadhaar misuse (2017-2025)

Year	Incident	Scale/ Impact	Key Vulnerability
Data Leak Incidents			
2017	CIS identified exposure of Aadhaar-linked data across four government/semi-public portals ³²⁴	Up to 135 million individuals	Public portal exposure, weak access controls
2017	Multiple government portals (KVIC, Kerala Sevana Pension, Egrantz, Telangana BC Welfare, Bihar & Punjab Minority Welfare, HRD) exposed Aadhaar-linked datasets ³²⁵	Thousands to lakhs of beneficiaries	Poor database governance, unsecured publication
2017	Jharkhand DSS pension portal exposed Aadhaar, bank details, and personal data due to a programming error ³²⁶	~1.4 million beneficiaries	Coding error, lack of audit controls
2018	Andhra Pradesh MGNREGA and housing portals exposed Aadhaar, bank details, caste, religion, geolocation ³²⁷	~89 lakh workers + 1.34 lakh beneficiaries	Excessive data disclosure, weak safeguards
2018	Kerala municipal/PMAY portals exposed Aadhaar-linked beneficiary data ³²⁸	1,783 beneficiaries	Portal misconfiguration
Security Vulnerability Cases			
2018	EPFO halted Aadhaar seeding via CSCs due to suspected vulnerabilities in portal ³²⁹	System-wide precautionary halt	Weak security architecture in service layer
2019	Indane/Indian Oil API leak exposed Aadhaar-linked customer data via unauthenticated API ³³⁰	~6.7 million records	API misconfiguration, lack of authentication
2023	Dark web listing claimed sale of Aadhaar-linked data of 815 million individuals (unverified) ³³¹	Claimed 815 million records	Potential large-scale aggregation risk (unconfirmed)

³²⁴ Aadhaar numbers of 135 mn may have leaked, claims CIS report. (2017). *The Times of India*.

<https://timesofindia.indiatimes.com/business/india-business/aadhaar-numbers-of-135-mn-may-have-leaked-claims-cis-report/articleshow/58529002.cms>

³²⁵ Iyer, N. (2017). #AadhaarLeaks: A list of Aadhaar data leaks. MediaNama. <https://www.medianama.com/2017/04/223-aadhaar-leaks-database/>

³²⁶ Details of over a million Aadhaar numbers published on Jharkhand govt website. (2017). Hindustan Times.

<https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFIScg5Dn5neLyBzrkW11.html>

³²⁷ Aadhaar data of over 89 lakh MNREGA workers in Andhra Pradesh leaked online. (2018). Centre for Internet and Society.

<https://editors.cis-india.org/internet-governance/news/new-indian-express-april-26-2018-aadhaar-data-over-89-lakh-mnrega-workers-in-andhra-pradesh-leaked-online> ; TNM Staff. (2018). Remove Aadhaar data from Andhra govt's portals, says UIDAI Chairman after data leak. The News Minute. <https://www.thenewsminute.com/andhra-pradesh/remove-aadhaar-data-andhra-govt-s-portals-says-uidai-chairman-after-data-leak-80993> ; AP government website leaks Aadhaar, caste, religion details of 1.3 lakh people. (2018). The New Indian Express. <https://www.newindianexpress.com/states/andhra-pradesh/2018/Apr/26/ap-government-website-leaks-aadhaar-caste-religion-details-of-13-lakh-people-1806590.html>

³²⁸ Express impact: Kozhikode Corporation removes Aadhaar data from its website. (2018). The New Indian Express.

<https://www.newindianexpress.com/states/kerala/2018/Jun/02/express-impact-kozhikode-corporation-removes-aadhaar-data-from-its-website-1822777.html>

³²⁹ EPFO suspends services through CSC, says no data leakage. (2018). India Today. <https://www.indiatoday.in/india/story/epfo-suspends-services-through-csc-says-no-data-leakage-1225340-2018-05-02>

³³⁰ Whittaker, Z. (2019). India's state gas company leaks millions of Aadhaar numbers. TechCrunch.

<https://techcrunch.com/2019/02/18/aadhaar-indane-leak/>

³³¹ Resecurity. (2023). PII belonging to Indian citizens, including their Aadhaar IDs, offered for sale on the dark web.

<https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web>

Identity Fraud			
2025	Multi-state racket manipulating biometrics and demographic data for Aadhaar updates ³³²	~1,500 identities affected	Insider misuse, weak operator controls
2020s	Fake Aadhaar cards created using publicly available Aadhaar numbers for schemes like PM-KISAN ³³³	Potential large-scale misuse	Data linkage + weak verification checks
2020s	Tamil Nadu case: forged PAN used to obtain Aadhaar for migrants/foreign nationals ³³⁴	100+ suspected cases	Identity verification loopholes
2020s	Rae Bareilly racket: Aadhaar operator credentials misused to generate fake Aadhaar and birth certificates ³³⁵	130+ fake IDs recovered	Credential compromise, insider risk
2020s	Dumping of 1,000+ Aadhaar cards in West Bengal raised concerns of fake identity circulation ³³⁶	1,000+ cards	Weak lifecycle management, verification gaps
Transaction Fraud			
2023–24	AePS fraud using cloned biometrics (e.g., copying thumb impressions from documents) ³³⁷	Increasing incidents; 11% of cyber frauds (I4C, 2024)	Biometric spoofing, device-level vulnerabilities
2020s	Gujarat case: Fingerprints of ~1,000 individuals used to siphon funds via AePS ³³⁸	~1,000 victims	Biometric cloning, weak endpoint security

³³² Rai, S. (2025). How UP-based gang tampered Aadhaar biometrics, altered thousands of digital identities across 12 states. The Times of India. <https://timesofindia.indiatimes.com/city/meerut/how-up-based-gang-tampered-aadhaar-biometrics-altered-thousands-of-digital-identities-across-12-states/articleshow/120072115.cms>

³³³ Sircar, S., & Sachdev, V. (2020). 'Riteish Deshmukh', Hanuman & Pak spy get PM KISAN cash as farmers. The Quint. <https://www.thequint.com/cyber/pm-kisan-scam-aadhaar-riteish-deshmukh-hanuman-pakistan-spy-get-cash-as-farmers>

³³⁴ Thomas, W. (2025). Efforts on to trace fraudulently obtained Aadhaar cards facilitated by Karur-based group. The Hindu. <https://www.thehindu.com/news/cities/Coimbatore/efforts-on-to-trace-fraudulently-obtained-aadhaar-cards-facilitated-by-karur-based-group/article69557839.ece>

³³⁵ Chakraborty, P. (2025). Fake Aadhaar racket busted in Rae Bareilly. The Times of India. <https://timesofindia.indiatimes.com/city/lucknow/fake-aadhaar-racket-busted-in-rae-bareilly/articleshow/125494565.cms>

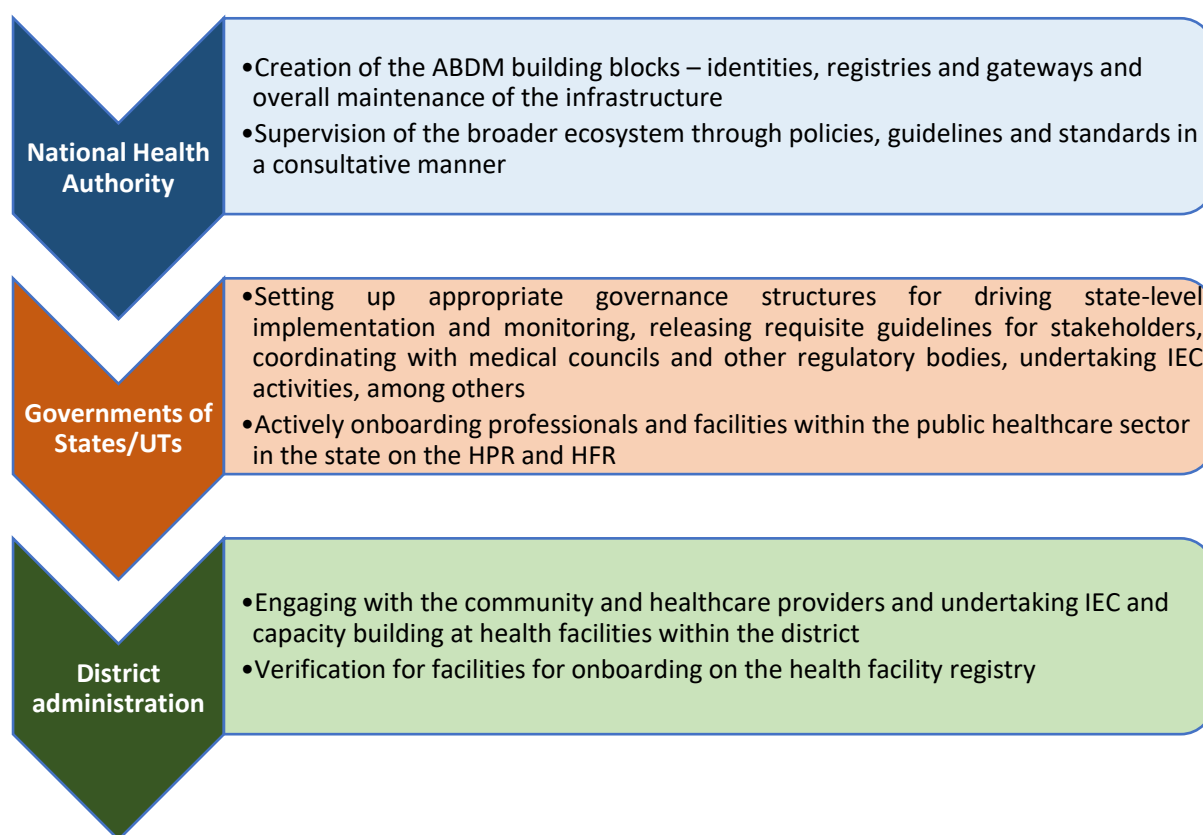
³³⁶ Shafiq, S. M. (2025). Over 1,000 Aadhaar cards found dumped in West Bengal pond; BJP alleges voter fraud, TMC dismisses as officials launch probe. The Logical Indian. <https://thelogicalindian.com/over-1000-aadhaar-cards-found-dumped-in-west-bengal-pond-bjp-alleges-voter-fraud-tmc-dismisses-as-officials-launch-probe/>; Zee Media Bureau. (2025). Fear of SIR? Thousands of Aadhaar cards found dumped in West Bengal lake; BJP blames Mamata Banerjee. Zee News. <https://zeenews.india.com/india/fear-of-sir-thousands-of-aadhaar-cards-found-dumped-in-west-bengal-lake-bjp-blames-mamata-banerjee-2980514.html>

³³⁷ Singh, V. (2024). Aadhaar-enabled payment comprised 11% of financial frauds: I4C analysis. The Hindu. <https://www.thehindu.com/news/national/aadhaar-enabled-payment-comprised-11-of-financial-frauds-i4c-analysis/article67706780.ece>

³³⁸ Tere, T. (2023). Aadhaar fingerprints used to siphon off bank money. The Times of India. <https://timesofindia.indiatimes.com/city/vadodara/aadhaar-fingerprints-used-to-siphon-off-bank-money/articleshow/98840920.cms>

Annexure 3: Ayushman Bharat Digital Mission (ABDM)

Figure 3.1: Roles and Responsibilities Across Various Levels of Government





Indian Council for Research on International Economic Relations (ICRIER)

Our Offices:

4th Floor, Core 6A, India Habitat Centre, Lodhi Road, New Delhi-110003

The Isher Building, Plot No. 16-17, Pushp Vihar, Institutional Area, Sector 6, New Delhi-110017

O: +91 11 43112400, **F:** +91 11 24620180 | **W:** www.icrier.org | **E:** info@icrier.res.in