INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

DIGITAL HEALTHCARE GOVERNANCE IN INDIA: A CRITICAL STUDY OF ABDM, PM-JAY, AND DATA PROTECTION LAWS

AUTHORED BY - SHIMONA S

Introduction:

Overview of Digital Health Technologies

The increasing use of digital tools such as health applications, data platforms, and information systems has fundamentally altered the organization and delivery of health services. These technologies support broader health system goals by improving access to affordable and high-quality care that is responsive to patient needs and aligned with the objective of Universal Health Coverage.

When health data is analysed and applied in a systematic and responsible manner, digital solutions can improve patient satisfaction, enhance the working conditions of health professionals, increase operational effectiveness, and contribute to improved clinical outcomes. In addition, digital health systems enable alternative approaches to service delivery and financing across both public and private health sectors.

Categories of Digital Health Records

Digital health information is stored in different formats, of which **Electronic Medical Records (EMRs)** and **Electronic Health Records (EHRs)** are the most prominent. Although these terms are often used interchangeably, they differ in purpose, scope, and the extent to which information is shared across institutions and levels of care.

Importance of Digital Health Records

Health-related data is now generated from multiple sources beyond traditional clinical settings. Information collected through wearable devices, mobile health platforms used by frontline health

workers, and advanced data sources such as genetic testing may be stored by entities that are not direct health care providers.

Digital health records should not be viewed merely as electronic substitutes for paper files. When they are designed with specific objectives, supported by reliable data, and accessible where and when needed, they can improve health system planning, resource allocation, service delivery, and disease prevention strategies. Conversely, digital record systems introduced without a clearly defined function often fail to demonstrate value and may become financially unsustainable.

Functional Advantages of Digital Health Records

Availability of Patient Information

- Ensures access to accurate and updated patient details during clinical encounters
- Enables controlled and secure exchange of health information

Documentation and Data Management

- Improves clarity and completeness of clinical records
- Supports efficient and accurate billing and coding practices
- Strengthens safeguards for data protection and confidentiality

Patient Involvement

- Facilitates timely communication between patients and health professionals
- Provides continuity of care for individuals with long-term health conditions
- Reduces repetitive data collection from patients

Clinical Effectiveness and Safety

- Incorporates decision-support mechanisms based on standard treatment protocols
- Improves long-term disease monitoring and patient adherence
- Decreases unnecessary investigations and procedures
- Allows uninterrupted access to patient data across locations and time
- Enhances coordination among health care providers
- Connects individual records to shared registries and databases

System-Level Efficiency

- Reduces administrative workload through automation
- Lowers expenditure by minimizing clinical errors and inefficiencies
- Encourages rational use of effective and affordable treatment options

Surveillance and Research

- Assists in early identification of disease trends and outbreaks
- Supports public health analysis and medical research

Concept and Scope of Digital Health Records

There is no single, universally accepted definition for terms such as electronic medical record, electronic health record, computerized patient record, personal health record, or shared health record. These concepts are interpreted differently across countries and health systems.

An **Electronic Medical Record (EMR)** refers to a digital file created by a health-related entity that documents patient-specific information over time. It typically includes personal details and clinical data required for diagnosis, treatment, follow-up, and referral. EMRs may also be generated by diagnostic laboratories, pharmacies, mobile health applications, and technology companies that collect and store individual health information.

Although additional contextual data—such as environmental exposure or socio-educational background—may influence health outcomes, such information is generally not classified as part of an EMR.

An **Electronic Health Record (EHR)** represents a broader system that combines data from multiple EMRs and other digital sources. Due to the technical complexity and financial investment required, EHR systems are usually implemented by large health organizations, integrated care networks, or government authorities. In some regions, EHRs are designed to operate beyond national borders. For example, European initiatives aim to enable the sharing of patient records across different countries to support continuity of care.

In principle, an EHR is intended to reflect a person's complete health history, including clinical findings, test results, treatments, preventive services, and patient-reported activities. However, creating such an all-encompassing record is difficult in practice, as it requires extensive data integration. Without a clearly defined purpose, this level of integration is rarely cost-effective.

To address this challenge, several health systems have adopted **patient summary records**, which contain a limited but essential set of information. These typically include demographic data, diagnosed conditions, current medications, allergies, recent clinical procedures, and immunization history. Patient summary records are commonly used to support emergency and unplanned care by ensuring that critical information is readily available when needed.

Understanding EMR and EHR Information Systems

From a data-management perspective, **Electronic Medical Records (EMRs)** and **Electronic Health Records (EHRs)** function primarily as structured repositories of patient-related information. On their own, these records do not perform tasks or deliver services; rather, they serve as organized collections of health data that require supporting systems to become operationally useful.

According to the International Organization for Standardization (ISO), an **EHR system** is a comprehensive digital infrastructure consisting of multiple components. These include one or more data repositories, directory services that catalogue human and non-human resources, clinical knowledge services such as terminologies and care pathways, workflow engines, user-facing applications, reporting and analytics modules, and security mechanisms. The effectiveness of an EHR system depends not only on the presence of these elements but also on how they are structured and interconnected.

Data Integration and System Interoperability

In many health systems, information is stored in isolated and independent databases that frequently duplicate the same reference data. Examples include facility identifiers and locations, health worker registries, national medicine lists, and diagnostic classification codes. When such systems operate without interoperability, inconsistencies arise. Any update—such as a change in a facility's name or address—must be replicated across multiple platforms, increasing the likelihood of errors and outdated records. As a result, data becomes fragmented, partially accurate, and difficult to maintain, creating inefficiencies across the health information ecosystem.

Scope and Complexity of EMR and EHR Systems

The intended function of an EMR or EHR system directly influences its design and implementation complexity. Systems designed to operate across larger geographical areas or serve multiple functions typically require more sophisticated architectures. Similarly, implementation becomes more challenging in jurisdictions that are geographically extensive or administratively decentralized, as coordination across institutions and governance levels is required.

Stages of EHR System Development

The development of an EHR system can be broadly categorized into four sequential phases:

1. **Preliminary evaluation and agreement on objectives**
2. **Analysis of the existing environment**
3. **System design and architecture planning**
4. **Deployment and operational rollout**

Needs Assessment and Purpose Definition

The initial phase focuses on determining how EMR and EHR systems can support wider health system priorities, existing challenges, and long-term strategies, including national or regional digital health frameworks. A high-level needs assessment helps identify demand at the system level and clarifies the functional and geographical scope of the proposed system.

Although evidence suggests that EMR and EHR adoption can improve health system performance, their design does not always align with broader policy goals or reform agendas. Therefore, early-stage planning must consider:

- Consistency with national and subnational health objectives
- Compatibility with ongoing health sector reforms

To support this phase, it is recommended to establish a multidisciplinary planning committee representing all major stakeholders. The responsibilities of such a body typically include:

- Identifying strategic priorities, short-term objectives, and operational requirements
- Guiding discussions on system goals and functional expectations
- Recommending policy frameworks and implementation strategies
- Acting as a communication bridge among stakeholders
- Promoting system adoption and awareness of its benefits
- Ensuring inclusive, participatory decision-making throughout the process

System Implementation Approach

Effective implementation requires allowing health professionals adequate time for training, supervised system use, and structured feedback. Introducing the system in stages enables users to adapt gradually while identifying areas for refinement.

A phased rollout also facilitates knowledge transfer. Individuals involved in early implementation—such as clinicians, technical staff, and trainers—can later support other

institutions, creating both formal and informal professional networks that encourage collaboration, problem-solving, and innovation.

Implementation Challenges and Constraints

The deployment and sustained operation of EMR and EHR systems demand substantial financial, technical, and human resources. Implementation is typically lengthy and involves multiple stakeholders, often extending over several years.

Comprehensive financial planning is essential, covering not only initial infrastructure investments but also recurring costs related to maintenance, system upgrades, and user support. In settings where foundational digital infrastructure—such as reliable electricity or broadband connectivity—is inadequate, additional investments are required, which must be aligned with broader digital development goals.

EHR systems are often large-scale and interconnected with numerous registries, platforms, and health applications. Given the sensitivity of health data and the scale of operations, risk assessment and mitigation strategies are critical. These systems carry significant financial, operational, and human implications.

A common limitation observed in many implementations is the underestimation of workforce-related challenges. Governments and health organizations frequently prioritize technical and financial considerations while overlooking issues such as insufficient digital literacy, resistance to change, and inadequate training among users.

Secure Management of Electronic Health Records

Secure electronic health record management systems are designed to protect databases containing sensitive personal and medical information. Their primary objective is to ensure confidentiality, data integrity, and controlled access, thereby reducing the risk of unauthorized use or data breaches.

Electronic Health Record Standards in India

In September 2013, the Ministry of Health and Family Welfare (MoHFW) formally introduced **Electronic Health Record Standards for India**. These standards emphasized alignment with internationally recognized frameworks to promote interoperability and consistency. Updated

standards were subsequently released in 2016 to support national-level digital health system implementation.

The MoHFW has actively encouraged adoption by making standardized clinical terminologies, including Systematised Nomenclature of Medicine–Clinical Terms (SNOMED CT), freely available in India. An interim National Release Centre has been established to manage and oversee clinical terminology standards.

Through these initiatives, the government aims to regulate the storage and exchange of electronic health data, strengthen privacy and security safeguards, and promote uniform adoption of e-health standards across the country. Increasing recognition of these standards by global health IT stakeholders reflects India's commitment to developing a structured, secure, and interoperable digital health ecosystem.

Selection and Evolution of Electronic Health Record Standards

The standards included in the notified framework were selected after reviewing internationally recognised Electronic Health Record (EHR) standards and evaluating their relevance and adaptability to Indian healthcare conditions. Emphasis was placed on identifying globally accepted practices that could be realistically implemented within India's legal, technical, and institutional context.

The committee entrusted with recommending these standards comprised a diverse group of stakeholders, including domain experts, healthcare practitioners, policymakers, technical specialists, and representatives from the health IT industry. The notified standards received broad support not only from professional and regulatory bodies but also from multiple stakeholders and independent technical and social analysts, who viewed the initiative as a positive and necessary reform.

Following notification, the Ministry of Health and Family Welfare (MoHFW) actively promoted implementation measures. Over the subsequent years, the Ministry facilitated access to internationally accepted standards such as SNOMED CT by making them freely available nationwide. Additionally, an interim National Release Centre (NRC) was established to manage and oversee this clinical terminology, which has gained increasing acceptance among global healthcare IT communities.

At the time of notification in September 2013, it was clearly recognised that EHR standards are dynamic in nature and would require periodic updates. Accordingly, MoHFW constituted an expert review group to reassess the previously notified standards based on implementation experience and anticipated future requirements. The revised standards presented reflect the outcome of extensive deliberations, including a detailed review of open standards and compliance with guidelines issued by the Ministry of Electronics and Information Technology (MeitY), Government of India.

Rationale for Adopting Electronic Health Records

Throughout an individual's lifetime, every interaction with the healthcare system generates a clinical record that represents a health-related event. While some of these records may appear insignificant in isolation, they can become clinically relevant depending on future health conditions. Therefore, it is essential that such records are preserved, chronologically organised, and clinically meaningful to provide a comprehensive overview of an individual's health history.
In the absence of standardisation, the creation of a lifelong health record is impractical. Medical data generated over several decades, often across multiple institutions and formats, cannot be meaningfully integrated without predefined rules for data capture, storage, retrieval, exchange, and analysis. Standardisation must encompasss not only textual data but also clinical codes, diagnostic images, and structured datasets.

Objectives of EHR Standardisation

The principal aims of implementing standards for electronic health record systems include:

- Enabling interoperability and, where required, specifying content exchange formats and clinical vocabularies to support semantic consistency
- Ensuring continued development and timely revision of adopted standards
- Encouraging innovation through the use of standardised technical frameworks
- Promoting widespread adoption by vendors, providers, and stakeholders
- Minimising implementation and operational costs wherever feasible
- Incorporating established best practices, policy frameworks, and experiential learning
- Preferring modular standards that function independently rather than being tightly coupled.

Patient Identification Requirements

An electronic health record system must support the inclusion of patient identifiers, prioritised as follows:

1. Aadhaar number issued by UIDAI, wherever available
2. In the absence of Aadhaar, a combination of locally assigned identifiers as used by the healthcare service provider

Technical Infrastructure Guidelines

Hardware Requirements

- IT infrastructure should meet or exceed the specifications required by the deployed software systems
- All medical and IT equipment must comply with applicable standards issued by BIS, NEMA, IEEE, ISO, CE, RoHS, EnergyStar, and relevant medical device regulations
- Adequate data backup and preservation mechanisms must be implemented, with storage capacity planned in accordance with legal requirements
- System redundancy should be built into critical components such as storage, power supply, and network connectivity
- Network security controls must be implemented and periodically audited
- Hardware systems should be routinely evaluated to ensure proper functioning
- Capacity planning and periodic upgrades must align with organisational quality and performance needs

Networking and Connectivity

- Systems should support multiple connectivity options, including internet-based networks, LAN, WAN, mobile technologies, and cloud platforms, to enable integration of multiple EMRs into a unified lifelong record
- Connectivity solutions must be reliable and sufficiently fast to support secure data exchange without degrading user experience
- Data transmission must ensure authenticity, non-repudiation, and protection against unauthorised alteration
- Continuous data integrity must be maintained during exchange and storage

Privacy, Security, and Trust Framework

For the purposes of these standards:

- **Privacy** refers to restricting access to health data solely to individuals or organisations authorised by the patient
- **Security** involves protecting personal health data from unauthorised access, particularly during electronic transmission
- **Trust** requires verification that users and institutions are legitimately who they claim to be

Electronic Protected Health Information (ePHI) includes any health-related data that is created, stored, transmitted, or received in electronic form.

Under the Information Technology Act, 2000, and its associated rules, protection extends to both personal information (PI) and sensitive personal information (SPI), with SPI forming a specific subset of PI. Sensitive personal data includes, among others:

- Authentication credentials
- Financial details
- Physical and mental health information
- Sexual orientation
- Medical records and history
- Biometric identifiers

Ownership of Health Data

- Medical records generated by healthcare providers are held in trust on behalf of the patient
- The health information contained within such records is owned by the patient
- Storage and transmission infrastructure remains the responsibility of the healthcare provider
- Ownership of sensitive personal and personal information remains with the patient, as defined under applicable law

Disclosure of Protected Health Information

- For treatment, billing, and healthcare operations, general patient consent is required
- For non-routine or non-healthcare uses, explicit and specific consent must be obtained
- Disclosure without prior consent is permitted where mandated by law, including for notifiable diseases or national priority programs

- Disclosure without authorisation is also permitted in cases involving court orders or fully anonymised datasets

Obligations of Healthcare Providers

Healthcare providers are required to:

- Secure stored health information in accordance with prescribed guidelines
- Remove identifying details when disclosure does not require patient identification
- Inform patients of their rights regarding health data privacy
- Develop, document, implement, and audit privacy policies
- Provide regular privacy and security training to staff

Rights of Patients and Legal Representatives

Patients or their authorised representatives may:

- Request copies of medical records, to be provided within 30 days
- Restrict disclosure of specific information either temporarily or permanently
- Obtain detailed logs of record disclosures, including date, recipient, content, and purpose

Grounds for Denial of Information

Access to records may be restricted where disclosure could pose a risk to the safety of the patient or others. This includes:

- Information obtained under confidentiality agreements
- Psychotherapy notes
- Records prepared for legal proceedings

Preservation of Electronic Medical Records

Electronic health records must be preserved for the lifetime of the individual and must not be destroyed. Following death, records may be transitioned to inactive status once legal proceedings conclude. Healthcare providers are encouraged to retain records indefinitely due to their relevance for genetic, familial, and public health research. Advances in data storage technologies make long-term preservation economically feasible.

Identifiable Health Information

Health data is considered identifiable if it includes elements such as names, addresses, contact details, identification numbers, biometric data, images, voice recordings, or any combination of attributes that can reasonably identify an individual.

Applicable Legal Framework

All provisions are subject to prevailing Indian laws, including the Information Technology Act, 2000, and subsequent amendments.

Security of Electronic Health Information

Healthcare entities must adopt administrative, physical, and technical safeguards to ensure confidentiality, integrity, and availability of ePHI. Security controls should be proportionate to organisational size, technical capability, cost considerations, and risk exposure.

Authentication mechanisms must verify user identity and authorisation both locally and across networks. Automatic log-off mechanisms should terminate inactive sessions while preserving unsaved user data for usability.

Ayushman Bharat Digital Mission (ABDM): Overview

The Ayushman Bharat Digital Mission, launched in 2021, aims to establish a unified digital health ecosystem by assigning digital health identifiers to citizens. Implemented by the National Health Authority under MoHFW, the mission operates as a centrally sponsored scheme with a five-year duration.

ABDM seeks to integrate hospitals, insurers, healthcare professionals, and patients through interoperable digital platforms. Participation is voluntary for healthcare institutions. Applications such as ABHA and Aarogya Setu support record storage and provider connectivity. The scheme has been allocated ₹1,600 crore for implementation between 2021–2026 and has achieved substantial national coverage, with hundreds of millions of health accounts, linked records, verified facilities, and registered healthcare professionals.

Digital Transformation of Healthcare in India

Healthcare systems across the world are undergoing a profound transformation driven by advancements in digital technology. India, with its vast population and diverse healthcare needs, has increasingly turned towards digital solutions to address long-standing issues of accessibility, efficiency, transparency, and continuity of care. In this context, the Ayushman Bharat Digital Mission (ABDM) represents a landmark policy initiative aimed at creating an integrated digital

health ecosystem that connects individuals, healthcare providers, and governing institutions through interoperable digital infrastructure.

The ABDM seeks to move beyond fragmented and paper-based systems by enabling seamless creation, storage, access, and exchange of health-related information. By leveraging digital platforms, the mission aims to ensure that healthcare delivery becomes more patient-centric, data-driven, and accountable. At its core, ABDM is designed to empower individuals, streamline healthcare processes, and strengthen governance mechanisms through secure and standardised digital tools.

Core Architecture of the Ayushman Bharat Digital Mission

The design of ABDM rests on a set of foundational components that collectively enable interoperability, transparency, and secure data exchange. These components function as building blocks that support the broader vision of a unified digital health ecosystem.

Unique Digital Health Identification

A central element of the ABDM framework is the provision of a unique digital health identifier to every individual. Known as the ABHA (Ayushman Bharat Health Account) ID, this identifier allows individuals to digitally link their health records across multiple healthcare providers and platforms.

The ABHA ID serves several purposes. It ensures accurate identification of patients, reduces duplication of records, and facilitates continuity of care across institutions. Importantly, the use of this identifier is voluntary and consent-based, reinforcing the principle that individuals retain control over their personal health informati

Registry of Healthcare Professionals

To ensure trust and accountability within the digital health ecosystem, ABDM incorporates a comprehensive registry of healthcare professionals. This registry includes practitioners from both modern and traditional systems of medicine, thereby recognising India’s pluralistic healthcare structure.

The Healthcare Professionals Registry (HPR) acts as an authenticated database that enables professionals to participate in the digital health ecosystem. By linking verified credentials with

digital platforms, the registry helps prevent impersonation, enhances professional accountability, and facilitates secure interactions between providers and patients.

National Health Facility Database

Another critical pillar of ABDM is the creation of a centralised repository of health facilities across the country. This Health Facility Registry (HFR) includes both public and private institutions such as hospitals, clinics, diagnostic laboratories, imaging centres, and pharmacies.

The HFR functions as a verified source of information regarding healthcare establishments. By standardising facility-level data, it supports service discovery, regulatory oversight, and integration with digital platforms. Healthcare facilities registered under the HFR gain access to ABDM-enabled services, enabling seamless interaction with patients and other stakeholders.

Unified Health Interface

The Unified Health Interface (UHI) represents an innovation in service delivery by enabling discovery and access to healthcare services through interoperable digital applications. Rather than relying on isolated platforms, UHI allows multiple applications to connect within a common framework.

Through UHI-enabled systems, individuals can search for healthcare services, schedule consultations, and access digital health tools. This approach promotes competition, innovation, and user choice while maintaining standardisation and interoperability across platforms.

Data Protection and Information Security

Given the sensitive nature of health information, ABDM places significant emphasis on data security and privacy. The mission aligns its data governance framework with India's evolving data protection regime, particularly the Digital Personal Data Protection Act, 2023.

ABDM adopts a consent-based architecture where individuals explicitly authorise access to their health data. Advanced security mechanisms such as encryption, authentication protocols, and audit trails are incorporated to minimise risks of unauthorised access or data breaches.

Transparency and Accountability Mechanisms

Transparency is a key objective of ABDM. By enabling individuals to access information related to healthcare services, pricing, and provider credentials, the mission seeks to enhance accountability within the healthcare system.

Digital records reduce opportunities for manipulation or loss of information, while standardised protocols ensure compliance with clinical and administrative guidelines. This contributes to a more trustworthy and equitable healthcare environment.

Flagship Initiatives under ABDM

To operationalise its objectives, ABDM has introduced several targeted initiatives aimed at improving efficiency, adoption, and accessibility.

QR-Based Outpatient Registration

One of the most visible initiatives is the "Scan and Share" system for outpatient department (OPD) registration. Through this mechanism, patients can scan QR codes displayed at healthcare facilities and digitally share basic demographic details.

This reduces administrative delays, minimises manual data entry errors, and shortens waiting times. The initiative has proven particularly effective in high-volume public hospitals where patient queues have traditionally been long.

Incentivising Digital Adoption

Recognising the financial and operational challenges associated with digital transformation, the Digital Health Incentive Scheme (DHIS) has been introduced to encourage adoption among healthcare providers.

Under this scheme, hospitals, laboratories, and digital health solution providers receive incentives for adopting ABDM-compliant systems. This approach seeks to offset initial costs and promote long-term sustainability of digital health infrastructure.

Facilitating Private Sector Participation

To address adoption barriers within the private healthcare sector, ABDM has operationalised specialised microsites that offer onboarding support and technical guidance. These microsites function as resource hubs, assisting providers in navigating regulatory and technical requirements. The success of these initiatives highlights the importance of targeted engagement strategies in promoting widespread adoption across diverse stakeholders.

Comprehensive Adoption Pilots

ABDM has also undertaken pilot projects aimed at achieving end-to-end digitisation of healthcare facilities. These pilots establish model institutions that demonstrate best practices in digital health implementation, serving as benchmarks for future expansion.

Development of Sector-Specific Portals

In addition to healthcare delivery platforms, ABDM supports the creation of specialised portals such as the National Medical Register and National Dental Register. These portals enhance professional regulation, data accuracy, and institutional transparency.

Measurable Achievements of ABDM

Since its launch, ABDM has recorded significant progress across multiple indicators.

Expansion of Digital Health Accounts

By September 2024, a substantial proportion of India's population had created ABHA IDs. These accounts enable individuals to securely access and share health records, contributing to improved continuity of care.

A large volume of health records has been digitally linked, demonstrating increasing acceptance of digital record-keeping among healthcare providers and patients alike.

Ecosystem Integration

The integration of numerous private entities, including diagnostic laboratories, pharmacies, and health technology companies, reflects the growing interoperability of the ABDM ecosystem.

Leading public institutions have also demonstrated high adoption rates, reinforcing the credibility of the system.

Registry-Based Governance

The National Healthcare Providers Registry has enabled large-scale registration of healthcare facilities and professionals. This consolidated database supports regulatory oversight, service planning, and policy formulation.

Persistent Challenges in Implementation

Despite its achievements, ABDM faces several structural and operational challenges.

Infrastructure and Connectivity Gaps

Digital health initiatives depend heavily on reliable internet connectivity and digital literacy. While urban regions have benefited from improved infrastructure, rural and remote areas continue to face limitations that hinder effective engagement with digital platforms.

Data Privacy and Cybersecurity Risks

The scale of digital health data raises concerns regarding privacy, cybersecurity, and misuse. Effective consent management and robust enforcement mechanisms remain critical to maintaining public trust.

Financial and Capacity Constraints

Smaller healthcare facilities often lack the resources required for digital adoption. High implementation costs, coupled with limited technical expertise, pose barriers to universal participation.

Legal and Regulatory Uncertainty

The evolving nature of digital health regulation has created ambiguity regarding data ownership, liability, and accountability. Clear and harmonised legal frameworks are necessary to support sustainable growth of digital health systems.

Personal Health Records within ABDM

Personal Health Records (PHRs) represent a paradigm shift in health data management by placing individuals at the centre of information control. Unlike institutional records, PHRs are managed and accessed by individuals themselves.

ABDM-enabled PHR applications allow users to consolidate records from multiple healthcare providers, creating a longitudinal view of their health history.

PHRs enhance patient autonomy by enabling individuals to decide how, when, and with whom their health information is shared. This consent-driven model strengthens trust and aligns with constitutional principles of privacy.

By providing healthcare providers with access to comprehensive patient histories (subject to consent), PHRs support informed decision-making, reduce duplication of tests, and improve treatment outcomes.

Regulatory and Legal Framework Governing Digital Health

India's digital health landscape is governed by a combination of sector-specific and general laws.

Information Technology and Data Protection Laws

The Information Technology Act, along with associated rules on sensitive personal data, provides foundational protections for electronic health information. The Digital Personal Data Protection Act, 2023, further strengthens accountability and governance mechanisms.

Professional conduct regulations, clinical establishment laws, and medical device rules collectively shape the regulatory environment for digital health services.

Intellectual Property Considerations

Patent and copyright laws play a significant role in shaping innovation within the digital health sector. While software-based innovations face restrictions under patent law, judicial interpretations have allowed protection where technical contributions are demonstrated.

Liability and Consumer Protection

Adverse outcomes arising from digital health solutions may attract civil or criminal liability. Consumer protection laws provide remedies for negligence, while professional ethics bodies address misconduct by healthcare practitioners.

Future Directions and Policy Recommendations

Targeted investments in connectivity and digital literacy, particularly in rural areas, are essential for inclusive adoption of ABDM.

Comprehensive consent frameworks, cybersecurity protocols, and enforcement mechanisms must be prioritised to safeguard sensitive health data.

Sustained funding, technical assistance, and training programmes can support smaller healthcare providers in adopting digital systems.

Clear definitions of data ownership, accountability, and liability will strengthen trust and facilitate long-term sustainability of the digital health ecosystem.

Conclusion:

The Ayushman Bharat Digital Mission represents a transformative step in India's healthcare governance. By integrating digital identification, interoperable platforms, and patient-centric data management, ABDM seeks to address long-standing inefficiencies and inequities in healthcare delivery.

While challenges related to infrastructure, regulation, and trust remain, the mission's comprehensive architecture and evolving policy framework provide a strong foundation for future growth. With sustained commitment and inclusive implementation, ABDM has the potential to redefine healthcare access, quality, and accountability in India.