



Consultation Paper
on
Proposed Health Data Retention Policy

9th Floor, Tower - 1
Jeevan Bharati Building,
Connaught Place
New Delhi - 110001

Written Comments on the Consultation Paper are invited from the stakeholders by 24th December 2021. Comments are to be preferably posted electronically on the ABDM website via the form available at <https://abdm.gov.in/publication/consultationpapers>. The comments could also be sent to Shri Kiran Gopal Vaska, Joint Director (Coordination), National Health Authority, on the email ID abdm@nha.gov.in. For any clarification/ information, he may be contacted at Telephone No. 011-23468703

Acronyms and Abbreviations

ABDM	Ayushman Bharat Digital Mission
API	Application Programming Interface
EHR	Electronic Health Records
EMR	Electronic Medical Records
HFR	Health Facility Registry
HID	Health ID
HIP	Health Information Provider
HIU	Health Information User
HPR	Healthcare Professionals Registry
HRP	Healthcare Repository Provider
ICT	Information Communication & Technology
MoHFW	Ministry of Health and Family Welfare
NABH	National Accreditation Board for Hospitals & Healthcare Providers
NABL	National Accreditation Board for Testing and Calibration Laboratories
NDHB	National Digital Health Blueprint
NDHE	National Digital Health Ecosystem
NHA	National Health Authority
NHP	National Health Policy
PHI	Personal Health Information
PHR	Personal Health Records
PII	Personally Identifiable Information

Table of Contents

Executive Summary	6
Chapter 1: Introduction and Background of the Consultation Paper.....	8
1.1 Background.....	8
1.2 Objectives.....	8
1.3 Scope of Consultation Paper.....	9
1.4 Consultation Process.....	10
1.5 Evolution of ABDM.....	10
1.6 Envisioned ABDM Architecture	11
1.7 Pilot of ABDM Building Blocks	12
Chapter 2 – Need for Health Data Retention Guideline/Policy	15
2.1 Importance of Health Data Retention	15
2.2 Existing Guidelines for Health Data Retention in India	16
2.3 Relevance within ABDM	18
2.4 Key Issues for Consultation	20
Chapter 3 - Scope of the Health Data Retention Guideline/Policy.....	21
3.1 Stakeholders	21
3.2 Key Issues for Consultation	22
Chapter 4 – Key Elements for Health Data Retention	24
4.1 Retention Duration for Health Data.....	24
4.2 Storage and Maintenance of Health Data Retention.....	25
4.3 Data Classification for Health Data.....	26
4.4 Anonymization and Pseudonymization.....	30
4.5 Country Comparison on Data Retention.....	31
4.6 Use cases as per requirement of the health record in India	36
4.7 Existing Implementation of Guidelines for Retention of Health Records in India ..	36
4.8 Key Issues for Consultation	37
Chapter 5 - Proposed Approach for Health Data Retention Guideline/Policy	39
5.1 Proposed Classification	39
5.2 Proposed Duration by Health Data Type	40

5.3 Mode of Health Data Retention	40
5.4 Proposed Health Data Retention Governance Structure	41
5.5 Key Issues for Consultation	41
Annexure	42
List of Questions.....	42
Disclaimer.....	44

Executive Summary

The purpose of formulation and implementation of a Health Data Retention Guideline/Policy¹ for India is to ensure uniformity in a manner, which ensures that every healthcare facility implements record retention and compliance with all applicable regulations / guidelines / laws in India.

The proposed Health Data Retention Guideline/Policy has been envisioned to minimize risks associated with personal health data and to maximize benefits from usage of this data by ensuring that data retention guidelines are in sync with all applicable legal and regulatory compliances.

Several lines of evidence show that nations, which have developed strong health data governance systems, have safely and securely used health data for strengthening healthcare / public health delivery systems^{2,3,4,5,6}.

India's healthcare ecosystem shall benefit from this policy under ABDM. In order to ensure that health data of individuals is available for a pre-determined period of time as required by the ecosystem, this consultation paper covers in detail varied viewpoints across the chapters, including contextual requirements and use cases while weighing in the benefits for better health outcomes via a Health Data Retention Policy, which may be governed by ABDM.

¹ **The term guideline and policy for health data retention has been used interchangeably in the document. The document is only at consultation stage and the final decision shall be taken after feedback from stakeholders.**

² eHealth Network (2015). Governance model for the eHealth Digital Service Infrastructure during the CEF funding. Available at:

https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co02_en.pdf

³ 5 Research2Guidance (2018). Digital Diabetes Care Market 2018-2022. Available at:

<https://research2guidance.com/wp-content/uploads/2018/08/R2G-Digital-Diabetes-Care-Market-2018-2022-Ready-To-Take-Off-Report-Preview.pdf>

⁴ ESPON Future Digital Health in the EU Scientific Access. Available at:

https://www.espon.eu/sites/default/files/attachments/Scientific%20annexes.%20TG%202019%2003%2025_final%20version_0.pdf

⁵ EU2017.ee (2017). Estonia's unique e-health: thousands of data fields, one personal health record.

Available at: <https://www.eu2017.ee/news/press-releases/estonias-unique-e-health-thousands-datafields-one-personal-health-record>

⁶ Kauppinen, H., Ahonen, R., Mäntyselkä, P., Timonen, J. (2017). Medication Safety and the Usability

of Electronic Prescribing as Perceived by Physicians - A Semistructured Interview among Primary Health Care Physicians in Finland. *Journal of Evaluation in Clinical Practice*, 23, 1187-1194.

Chapter 1 highlights the objectives of this consultation paper giving us a background on ABDM and its scope, as well as the importance of data management policies from which a need arises for further exploring applicable data retention policy.

Chapter 2 lays the context, importance, and existing landscape for health data retention while explaining the relevance and need for a new policy for India to be supported under Ayushman Bharat Digital Mission (ABDM).

Chapter 3 lays out the scope of the health data retention policy. In this regard, detailed emphasis is laid on establishing the role of concerned stakeholders under the ambit of the policy, and whether the entire healthcare ecosystem or only entities part of ABDM should be covered by the policy being discussed.

Chapter 4 focuses on the different aspects such as the need to define retention duration, impact of short-term vs long-term retention of health data based on type of data. Data classification is discussed from both macro- and micro-level perspectives, and a cross-country comparison has also been discussed. This chapter also covers policy enforcement for applicable guidelines in the Indian context for certain use cases along with compliance to certain accreditations.

Chapter 5 covers a proposed approach for health data retention policy for India, pertaining to different data types, and also covers what suitable modes of retention could be considered. The proposed guidelines are aligned with the long-term horizon for better quality of healthcare delivery systems.

Finally, Annexure 1 provides a list of all consultation questions.

Chapter 1: Introduction and Background of the Consultation Paper

1.1 Background

In India, retention of health records by various healthcare entities and systems is governed by multiple guidelines as may be required to ensure compliance with an act, or an accreditation mandate, or organizational policy in force. Health facilities are obligated for maintenance and retrieval of any past records for future diagnosis or healthcare delivery activities. Henceforth, health facilities are following non-uniform retention duration across healthcare systems, which eventually does not benefit citizens due to fragmented record management practices of health records.

In the absence of a uniform guideline, and due to lack of understanding of implications of such fragmented retention approaches, realizing the goals of the Ayushman Bharat Digital Mission (ABDM) in facilitating long-term health benefits via quality, data-driven digital solutions would be challenging. The need for guidelines on data retention for personally identifiable information (PII), or personal health information (PHI) also stems from the emerging landscape and thinking and on the need for protection of sensitive data while ensuring effective usage of such information in clinical decision-making by healthcare professionals. This leads to improvement in overall quality of healthcare delivery and which is possible only if longer retention periods are mandated for certain types of health data discussed later in this paper.

Various existing guidelines discussed subsequently in this paper have been reviewed before writing this consultation paper; however, none provide a superseding directive covering the entire healthcare ecosystem in India.

1.2 Objectives

This consultation paper invites stakeholders' comments and feedback on developing a Health Data Retention Policy (HDRP) under the ambit of the Ayushman Bharat Digital Mission (ABDM), and to subsequently define the best practices required to be incorporated into the policy. Under ABDM, digital health records shall be maintained in a federated architecture. Furthermore, availability of this health data for ensuring continuity of care via interoperable systems is critical. Pursuant to the Health Data Management Policy, NHA is required to formulate a policy on health data retention to be adopted by the healthcare ecosystem in India and associated entities in the National Digital Health Ecosystem (NDHE).

As directed by Ministry of Health and Family Welfare (MoHFW), NHA is required to develop a policy covering detailed guidelines on health data retention and this policy may have

implication beyond the ABDM ecosystem. Through this consultation paper, the NHA is providing interested stakeholders with information that may be useful to understand the considerations for the proposed policy for India, and its related implications, and to seek their suggestions/inputs on health data retention under ABDM.

In this document, an attempt has been made to frame and contextualize the issues for consultation and provide adequate context for the public to weigh in with their comments. A wide range of policy, strategic, and technical matters are covered, some of which may depend upon legal interpretation. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. The approaches discussed henceforth are ideas and not decisions. Final decision shall be taken after considering suggestions and feedback received on this paper.

Multiple research studies have been reviewed for drafting this consultation paper and the information presented herein. This consultation is of high importance, and it shall enable ABDM to build a robust policy, which could become a uniform policy for adoption by the Indian healthcare ecosystem, beyond National Digital Health Ecosystem (NDHE) as well. This would benefit stakeholders by (i) providing clarity on how long retention duration for certain data types shall improve service delivery to patients and (ii) laying out the direction for ensuring compliance for retention.

NHA understands that there might still be gaps with respect to the research undertaken. Hence, the desired outcome from this process of consultation is to obtain clear feedback and answers to the questions posed at the end of each chapter. Additionally, stakeholders are welcome to raise any other issues they deem critical for the development of such a policy.

This consultation paper is restricted to the proposed Health Data Retention Policy of the Ayushman Bharat Digital Mission (ABDM). Information on other building blocks (Health Facility Registry (HFR), Healthcare Professionals Registry (HPR), United Health Interface (UHI), etc. and issues within them have been discussed in other consultation papers published by the NHA.

1.3 Scope of Consultation Paper

This paper focuses on the Health Data Retention policy within the ABDM ecosystem. It describes NHA's current approach related to data retention, and how a health data retention policy for ABDM stakeholders will help the healthcare ecosystem. Importantly, the Health Data Retention Policy is prospective, not retrospective.

ABDM is currently evaluating the most feasible option for laying down guidelines on Health Data Retention, and thus each section has specific open questions where feedback from stakeholders has been sought to ensure the proposed policy is beneficial to all parties and will help accelerate the adoption of digital health services in India.

The guidelines of the proposed policy, potential benefits to various ecosystem stakeholders, the approach towards designing the system and the governance for managing the systems are also covered, and open for comments and feedback.

1.4 Consultation Process

Prior to issuing this comprehensive consultation paper, ABDM has reviewed various aspects related to health data retention in India as well as globally, some of which are covered in the following sections. Based on the analysis of existing guidelines, international practices mentioned in the following sections, and internal analysis, this consultation paper has been prepared to seek inputs from stakeholders on specific issues raised henceforth.

1.5 Evolution of ABDM

1.5.1 The National Health Policy (NHP), published in 2017, has the following goal:

“The attainment of the highest possible level of health and wellbeing for all at all ages, through a preventive and promotive health care orientation in all developmental policies, and universal access to good quality health care services without anyone having to face financial hardship as a consequence.”

1.5.2 A key tenet of the NHP was the adoption of digital technologies in the healthcare ecosystem. To realize this goal, the Ministry of Health and Family Welfare (MoHFW) constituted a committee headed by Shri J. Satyanarayana to develop an implementation framework for the National Health Stack. This committee produced the National Digital Health Blueprint (NDHB), laying out the building blocks and a comprehensive action plan to holistically implement a nationwide digital health strategy.

1.5.3 To define the rationale, scope, and implementation arrangements of the framework of digital healthcare ecosystem laid out in the NDHB, Ayushman Bharat Digital Mission (ABDM), was then launched on August 15, 2020, with the following vision:

“To create a national digital health ecosystem that supports universal health coverage in an efficient, accessible, inclusive, affordable, timely and safe manner, that provides a wide-range of data, information and infrastructure services, duly leveraging open, interoperable, standards based digital systems, and ensures the security, confidentiality and privacy of health-related personal information.”

For more information on the framework and evolution of the ABDM, you can refer to the National Digital Health Blueprint document at <https://abdm.gov.in/home/ndhb>.

1.6 Envisioned ABDM Architecture

1.6.1 Going forward, ABDM aims to transform the way digital health services are rendered in India. In order to achieve this goal, a revised representation of the ABDM architecture is represented below. The aim of this architecture is to allow for interoperability of both health data and health services.

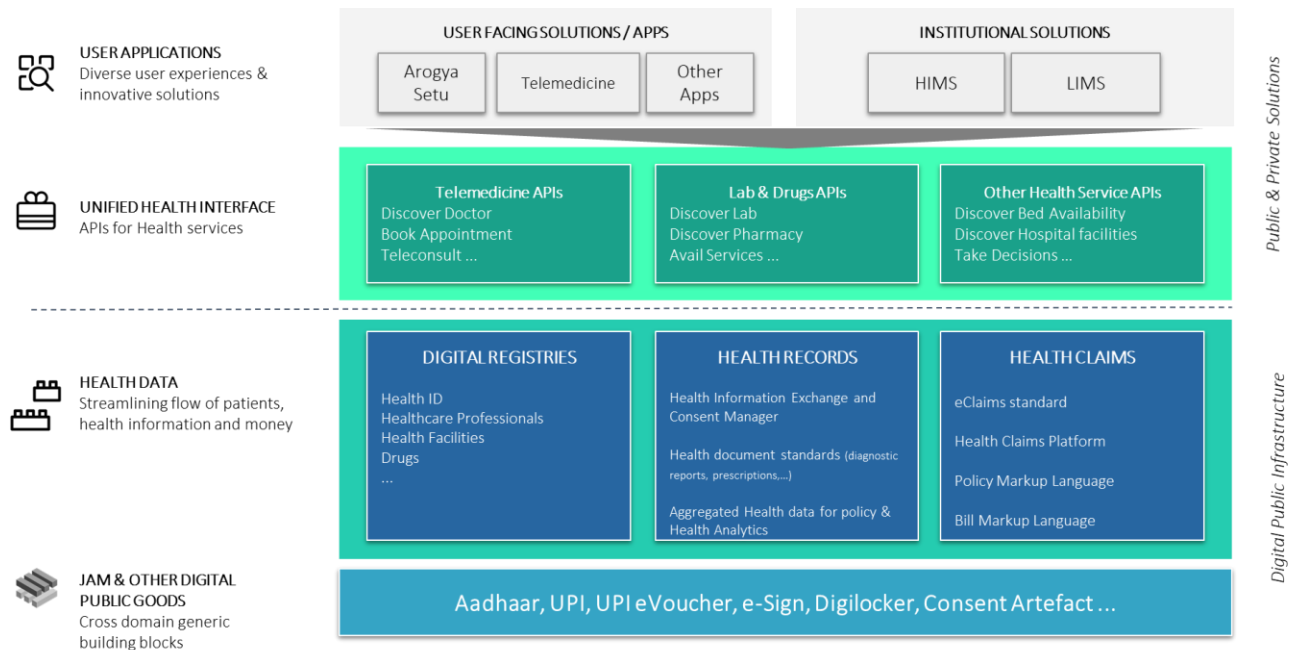


Fig. 1. Envisaged ABDM Architecture

1.6.2 The definitions and the envisioned functions of each of the layers is as mentioned below (the layers are described bottom-up)

- JAM and Existing Digital Ecosystems:** ABDM has been designed to operate effectively with, and leverage India's extant digital ecosystems, such as Aadhaar, Jan Dhan Bank Accounts, and Mobile (JAM), UPI, eSign, Digilocker, etc. These cross-domain capabilities are leveraged in ABDM to enable certain key functionalities such as (i) creation of a Health ID for individuals (ii) accessibility of digital health records through Digi Locker (iii) access to doctors and health facilities
- Health Data Exchange Layer:** This layer encompasses the core digital infrastructure modules needed to ensure the interoperability of health data. These building blocks include core registries - the Health ID, the Healthcare Professionals Registry and the Health Facility Registry, Health Information Exchange and Consent Manager, Health Data Standards (based on FHIR), coding terminology and data

aggregation specifications that drive trust and shareability of health data between patients and healthcare providers.

- 3. Health Services Layer:** Building blocks in this layer are envisioned to enable interoperable and seamless interactions between patients and providers of digital health services, and along with other ABDM building blocks to address challenges in delivering healthcare services digitally by creating an ecosystem that benefits both patients and providers.
- 4. User Applications:** This is the end-user layer of the ABDM ecosystem. It comprises the applications and platforms developed by the government or private sector through which patients, healthcare providers, insurers, researchers, policy makers, etc. access trusted health services. The application layer will interact with the health services and the health data layers thereby enabling health data exchange and a wide range of digital health services.

1.7 Rollout of ABDM Building Blocks

1.7.1 ABDM has been conceptualized as a set of “digital building blocks”. Each building block is seen as a “digital public good” that can be used by any entity in the digital health ecosystem and provides key capabilities that enable the ABDM Vision.

1.7.2 Since the announcement of ABDM, the National Health Authority (NHA) has launched the following key building blocks - Health ID, Personal Health Records (PHR) App, Healthcare Professionals Registry (HPR) starting with doctors, Health Facility Registry (HFR), and Health Information Exchange & Consent Manager (HIE-CM).

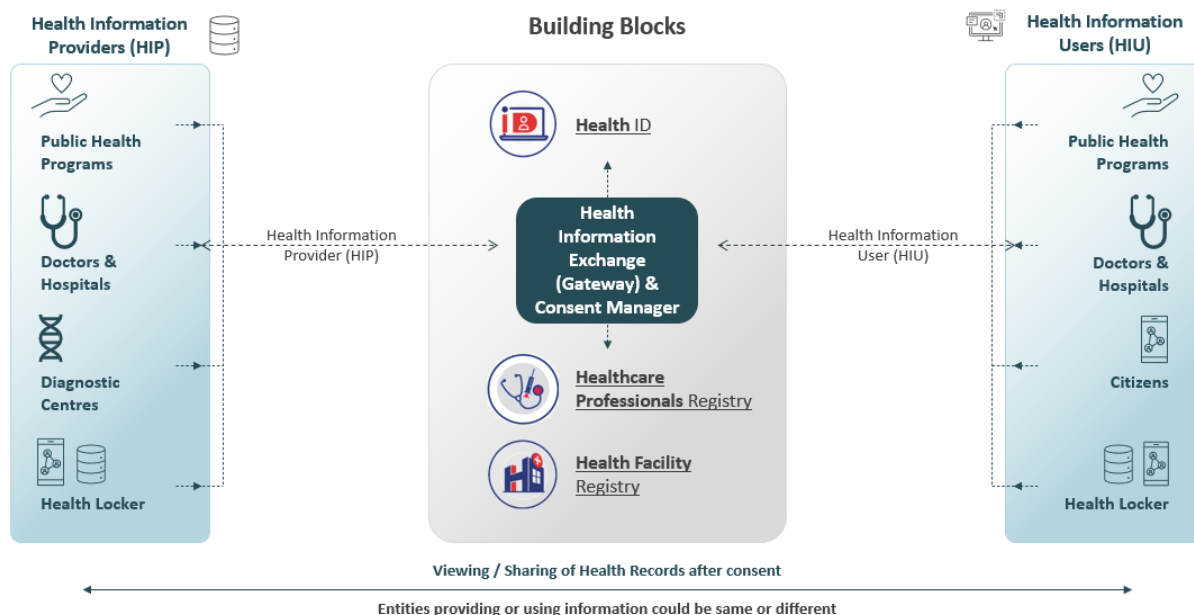


Fig. 2. ABDM Building Blocks

These building blocks are designed to enable identification of participating entities (health care providers, patients, and health professionals) and enable exchange of interoperable health data with patient consent. Any entity that wishes to share health information with a patient digitally in compliance with ABDM health standards is called a *Health Information Provider (HIP)* and any entity that seeks to access health data with consent is called a *Health Information User (HIU)*.

1.7.3 The ABDM building blocks have enabled new foundational capabilities including:

- A Health ID for every resident who wishes to obtain their health records digitally.
- Registered health facilities can link health records with Health IDs. This helps create a *longitudinal Personal Health Record (PHR)* for the individual, i.e., a medical record across multiple patient encounters at different health facilities.
- A consent mechanism to empower patients to access and share their PHR data. This mechanism is fully aligned with the draft Personal Data Protection Bill (2019)¹¹ of India.
- Standardization of the formatting of health records like diagnostic reports, discharge summaries, prescriptions, consultation notes and immunization records to make them interoperable. However, this standardization is not mandatory, and ABDM envisions the ecosystem to adopt standardization in order to garner the full benefits of technological flexibility.
- Digital identity for every verified healthcare professional and health facility who participates in ABDM.

Additional information on these building blocks and the pilot is available at <https://abdm.gov.in/>

1.7.4 The current ABDM building blocks have been built with the primary goal of ensuring the seamless interoperability of health-related data. Stakeholders in the ecosystem may use the ABDM APIs to access, share and verify health records, healthcare professionals and health facilities.

Chapter 2 – Need for Health Data Retention Guideline/Policy

This chapter provides background information on why a Health Data Retention Policy may be required as part of NDHE and sets the context for subsequent chapters. The relevance of health data retention in the context of the ABDM, Health Data Management Policy, and HIU/HIP guidelines have been discussed.

2.1 Importance of Health Data Retention

Data retention is the practice of storing and managing personal health data and records for a designated period and typically, the policies pertain to data type, format, duration, deletion mechanism, ownership, and procedure for violation or breach of the policy.

Healthcare organizations establish appropriate retention and archival or destruction schedules, to ensure the availability of timely and relevant data related to patient care, supported by robust life cycle of records management, which begins when information is created and ends when information is archived/destroyed. This ensures that patient diagnosis, prognosis, and health profiles are available for longer period, throughout patient lifetime or at least until completion of ongoing care delivery. These organizations, however, need a directive via necessary policies governing their practice of data retention.

The healthcare providers or labs create terabytes of data every year in the form of health records, lab results, and medical images. This data can be accessed by patients, government organizations, and doctors for healthcare decision-making after seeking patient's due consent. Thus, any such policy should cover the below requirements⁷:

- A system for compliance with data retention laws/rules/regulations etc.
- Ensuring availability of documents when needed
- Cost, time and space savings to balance storage, security, and infrastructure constraints of health facilities
- Protection against accidental loss or selective record destruction
- Schedule for destruction of non-relevant or obsolete documents

Traditionally retention functions have been managed using different media, including paper, images, optical disk, microfilm, DVD, and CD-ROM. The warehouses or resources from which to retrieve, store, and maintain data and information include, but are not limited to, application-specific databases, diagnostic biomedical devices, master patient indexes, and patient medical records and health information.

⁷ <https://library.ahima.org/PB/RetentionDestruction#.YQvD6l4zY2w>

Specifically, a record retention guideline should:

- Ensure patient health information is available to meet the needs of continued patient care, legal requirements, research, education, and other legitimate uses.
- Specify what information is kept, the time period for which it is kept, and the storage medium on which it will be maintained.
- Specify clear destruction policies and procedures, that include appropriate methods of destruction for each medium on which the information is maintained

2.2 Existing Guidelines for Health Data Retention in India

Patient health information is defined as Sensitive Data under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011⁸, but no guideline on retention schedule exists. In the absence of any superseding legislations or policies defined on health data retention in the country, many healthcare providers currently comply with self-prescribed standards applicable to their organization for storing, retaining, and maintaining applicable health records, which may cover compliance requirements per state, central or accreditation guidelines.

The MoHFW had notified the EHR Standards 2013 (revised in 2016)⁹, which are applicable for all Healthcare Providers, such that all electronic records must compulsorily be preserved and never destroyed during the lifetime of the person. With regards to ABDM, these standards could be adopted as a foundation for a policy on data retention, while considering a broader framework for the entire healthcare ecosystem.

With reference to the Indian healthcare regulations, a few other guidelines/policies exist in this regard. These have been reviewed thoroughly to understand how retention duration for health data types has been defined, to identify the gaps, and thereby propose a case for a new policy for ABDM stakeholders:

- **The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002**¹⁰ - These regulations prescribe that “every physician shall maintain the medical records pertaining to his / her indoor patients for a period of 3 years from the date of commencement of the treatment in a standard proforma laid down by the Medical Council of India”.

⁸ https://www.prsindia.org/sites/default/files/bill_files/IT_Rules_2011.pdf

⁹ Notification of Electronic Health Record (EHR) Standards - 2016 for India -reg

¹⁰<https://wbconsumers.gov.in/writereaddata/ACT%20&%20RULES/Relevant%20Act%20&%20Rules/Code%20of%20Medical%20Ethics%20Regulations.pdf>

- **The Clinical Establishments (Registration and Regulation) Draft Rules, 2010**¹¹ – The Draft Rules for Central Government suggest that medical records should be retained with the clinical establishment concerned for 3 to 5 years. The Act has taken effect in four States viz., Arunachal Pradesh, Himachal Pradesh, Mizoram, Sikkim, and all Union Territories, excluding the NCT of Delhi since 1st of March 2012, vide Gazette notification dated 28th February 2012. The States of Uttar Pradesh, Uttarakhand, Rajasthan, Bihar, Jharkhand, Assam, and Haryana have adopted the Act under clause (1) of article 252 of the Constitution of India.
- **Directorate General of Health Services for Central Government Hospitals in 2014**¹², in an Office Memorandum, stated that Medical Records of indoor patients may be stored in digitized form for at least 10 years or per availability. Hospitals can store hard copy of medical records – inpatient, OPD – 3 years; medico-legal registers and case sheets – 10 years or till the disposal of ongoing cases.
- The provisions of specific Acts like **The Pre-Conception Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994**, etc. necessitate proper maintenance of records that have to be retained for 2 years as specified in the Act.
- **The Personal Data Protection Bill, 2019**¹³ provides the provision that data can be stored only for as long as it is necessary to satisfy the purpose for which the data has been recorded by the entity.
- **Digital Information Security in Healthcare Act (DISHA)** was introduced in March 2019 by the Government of India to regulate ownership, collection, purpose, and storage of digital health data in alignment with the Electronics Health Records Standards of India (2016)¹⁴. Entities currently are highly restricted under DISHA, and are only permitted to generate, collect, and store health data for the following purposes¹⁵:
 - To advance the delivery of patient-centred medical care,
 - To provide information to guide medical decisions, or
 - To improve coordination of care and information among hospitals, laboratories, etc.

The approach considered in DISHA has been subsumed by the Personal Data Protection (PDP) Bill, 2019 to avoid duplicity of efforts.

¹¹ <http://www.clinicalestablishments.gov.in/cms/Home.aspx>

¹² <https://cghs.gov.in/index1.php?lang=1&level=2&sublinkid=7039&lid=4643>

¹³ <https://prsindia.org/billtrack/the-personal-data-protection-bill-2019>

¹⁴ <https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf>

¹⁵ Section 29(2), DISHA, 2018: *Purposes of collection, storage, transmission and use of digital health data*

2.3 Relevance within ABDM

As per the National Digital Health Blueprint, 2019 ("Blueprint") a federated architecture shall be adopted, for the management of digital health data to ensure interoperability across the National Digital Health Ecosystem.

2.3.1 Generation and Exchange of Health Records

Patient health data relating to an encounter or a set of encounters, is generated and maintained at the facility level (at the Point of Care) and would not be stored centrally. The health facility would be able to share the digitally created health records of patients with concerned doctors via EMR or HMIS solution, and in effect to the patients via a PHR Application, after patient's due consent. Health Information Exchange & Consent Manager (HIE-CM) shall enable the exchange of an interoperable health record for each individual by connecting the health information contained in various organizations across the entire continuum of care.

The current ABDM building blocks have been built with the primary goal of ensuring seamless interoperability of health-related data. Stakeholders in the ecosystem may use the ABDM APIs to access, share, and verify health records, healthcare professionals, and healthcare facilities.

ABDM building blocks are designed to enable identification of participating entities (health care providers, patients, and health professionals) and enable exchange of interoperable health data with patient consent.

2.3.2 HIP/HIU Guidelines

The HIP/HIU guidelines suggest that a healthcare provider who is creating health data (diagnostic reports, discharge summaries, prescriptions, etc.) digitally should be able to share these records with the patients, and also fetch records issued by other providers with user consent. To enable this, the hospital or the lab information management system need to be ABDM compliant, and will be required to modify and integrate their systems with ABDM building blocks and maintain health records of patients digitally to offer long term storage of health records on behalf of an HIP.

The primary requirement from an HIP is to ensure that:

- (1) All systems where data is maintained are up and running; and
- (2) Data is available for sharing and seamless exchange across applications as and when required.

2.3.3 Health Data Management Policy

ABDM has published the Health Data Management Policy (HDMP), and as per clause 6 it is required that a data retention policy is to be notified with adequate representation from all stakeholders involved in implementation of the ABDM.

The Health Data Management policy was approved (in December 2020) under ABDM to protect and manage personal data of patients using the digital services available in NDHE. The policy acts as a guidance document across NDHE, and sets out the minimum standard for data privacy protection that should be followed across the board to ensure compliance with relevant and applicable laws, rules, and regulations.¹⁶

The policy is dynamic in nature and subject to revision as may be required. Necessary guidelines with further consultation on scope for data retention guidelines shall be appended and issued for implementation within NDHE. The guidelines for the current policy shall be identified as required from this policy on health data retention under ABDM.

Clauses 14, 16.2, 19.2, 22.2 of Health Data Management Policy necessitates notification of a data retention policy. As per clause 26.6 any personal data collected will not be retained beyond the period necessary to satisfy the purpose for which it is collected and the data fiduciary will delete such personal data at the end of such processing in accordance with Clause 14 of HDMP as well as any guidelines relating to data retention and archival that may be notified from time to time.

The NDHE also enables service providers with health lockers to maintain and retain, health information generated by HIPs as well as any user uploaded records. A large hospital or a public health program (like RCH) could hold the records of patients in long term storage on premises or in the cloud. As per its own policies smaller diagnostic centers / clinics may use a specialized health repository provider who provides software solutions to help issue documents to patients and hold the same in long term storage.

As the policy guidelines are further being laid down, the current consultation on data retention rules and requirements shall help the ABDM receive clarity on roles and responsibilities of data fiduciaries and data processors with regards to retention schedules, business continuity to ensure the mandated duration and lifecycle of the records maintenance under all circumstances. Eventually, only this policy on data retention will be considered and adopted regarding applicable guidelines for retention of health records by all stakeholders under NDHE.

¹⁶ <https://www.insightsonindia.com/2021/01/21/rstv-the-big-picture-health-data-management-policy/#:~:text=Data%20collected%20across%20the%20National,Objectives%20of%20this%20Policy%3A&text=To%20ensure%20portability%20in%20the%20provision%20of%20health%20services>

2.4 Key Issues for Consultation

Health data retention under ABDM is a critical element for electronic record keeping by associated entities namely healthcare practitioner or health facility or any other public or private healthcare institution. There are benefits for retention as it facilitates better decision making for public health concerns, research at the State level.

Data retention requires ownership, maintenance, and regulated guidelines for enforcing a standardized approach via a common policy applicable for ABDM stakeholders, with recourse on any breaches. Thus, we invite concerned stakeholders to share their comments on below questions:

1. Whether there is a need for a Health Data Retention Policy and will Indian healthcare ecosystem benefit from such a Universal Data Retention Policy and what should be the key elements of this policy?
2. How should the guiding principle of this policy be determined for the benefit of stakeholders and ease of adoption by varying sizes of entities deciding to opt in for ABDM?

Chapter 3 - Scope of the Health Data Retention Guideline/Policy

In this chapter, the consultation paper outlines the envisaged scope of the Health Data Retention Guideline/Policy, and whether the scope should be applicable for the entire healthcare ecosystem in India, or if it should be limited to participating entities of NDHE. The advantages and disadvantages for each of the options, have also been introduced.

3.1 Stakeholders

3.1.1 Option 1 – Entire Healthcare Ecosystem in India

In this option, the policy scope shall include all healthcare facilities and associated entities in India who will adopt the data retention guidelines as defined, irrespective of their decision to opt-in or opt-out of NDHE.

Several entities who may not be covered, or those who may decide to opt out of the NDHE, including insurance providers, third-party administrators (TPA) offering individual and group insurance schemes, providers of open API systems, private PHR apps, teleconsultation platforms, data processors etc., will also be required to ensure that data retention guidelines are followed.

3.1.2 Option 2 – Healthcare entities opting-in for ABDM

In this option, the policy shall be applicable to only the health facilities and other entities opting in for ABDM. Any hospital, diagnostic center, clinic, public health program, etc. creating digital health records for patients can become an HIP or an HIU by signing up with the ABDM registries. The registry will issue them a digital key that needs to be configured in the application, being used by the facility, that is certified to be compliant with ABDM standards¹⁷ and the policy will be applicable for all types of health records generated via associated IDs pertaining to an individual.

The entities operating as part of ABDM, shall be responsible for ensuring that records are retained as per the predefined period under this policy.

Considering the above discussion, if Option 1 is adopted, it shall facilitate ease of opt-in and opt-out, and have a standardized approach to health data retention.

For either options, the policy would be applicable for all health records generated by the entities. However, to ensure that the policy is adopted, regulatory and legal

¹⁷ Guidelines for Health Information Providers, Health Repository Providers, Health Information Users and Health Lockers, ABDM

considerations shall be required. The details for both the options have been discussed further in this document.

3.1.3 Advantages and Disadvantages of each option

Scope	Advantages	Disadvantages
<p>Option 1</p> <p>Entire Healthcare Ecosystem in India</p>	<ul style="list-style-type: none"> The policy will provide a uniform approach towards health data retention enabling ease of adoption of any future policies/guidelines, reducing friction in any cases of opt-in/opt-out. 	<ul style="list-style-type: none"> Challenges maybe encountered in enforcement of the policy and it may be difficult for governing authorities to ensure adherence by each healthcare entity in the ecosystem
<p>Option 2</p> <p>Healthcare entities opting-in for ABDM</p>	<ul style="list-style-type: none"> As the scope shall be limited to entities opting-in for ABDM, it shall be easier to identify them and ensure that the policy is adopted along with other applicable guidelines for ABDM stakeholders, if any 	<ul style="list-style-type: none"> This might create subsystems within the larger healthcare ecosystem and may lead to a situation where entities not opting for ABDM continue with their non-standardised process of data retention If an entity opts out of ABDM, deletes all the health records, and later decides to opt-in again, the entity will still be in compliance of this policy. But the very purpose of this policy for ensuring long term authentic health records would not be fulfilled.

3.2 Key Issues for Consultation

The impact of the policy on different healthcare entities will be the deciding factor on the enforceability of the policy. The policy scope requires deliberation if it may be

applicable on the entire healthcare ecosystem requiring necessary capability, training, and suitable technologies to be implemented by all stakeholders, or it may be applicable only for healthcare entities participating in ABDM. With better understanding of available infrastructure, and readiness, the policy parameters can ensure suitable guidelines and uniform experience.

Thus, addressing the following questions would be helpful in building the scope and coverage of the policy:

1. As per Option 1, it has been proposed that the policy would be applicable to all healthcare entities from health data retention perspective. As per Option 2, the policy will be applicable only to entities participating in ABDM? Which would be a better option for the scope of the health data retention policy?
2. How such a policy should be implemented given limitations in terms of infrastructure, capability, and sufficient understanding of health data in the healthcare ecosystem?
3. As ABDM has a provision for opt-out, in such a scenario what may be the possible implications from the perspective of health data retention?

Chapter 4 – Key Elements for Health Data Retention

The proposed policy will consider two critical elements of data retention, i.e. duration of retention and data classification, to understand if different duration periods should be defined for different types of health records as may be feasible.

As retention schedules for very complex classification can be time consuming and resource intensive, it is important to evaluate the ideal minimum duration for each type of health data. Thus, this chapter is focused on the benefits of short-term vs long-term duration, types of health data collected, international comparison of data type as applicable, to evaluate and arrive at a proposed policy with retention schedules for each type of health data.

4.1 Retention Duration for Health Data

Globally, the requirement for health data retention policy stems from a country's personal data protection laws/legislations, which stipulates the requirement for personal health data as well. The retention schedules for personal health data retention, stem from the key principles of a country's data protection laws as maybe applicable at the state or federal levels.

There are no definite guidelines in India regarding how long health records should be retained since data protection guidelines are evolving.

As observed across multiple healthcare providers in India, a minimum of 3 years of retention period is adopted for personal health data to ensure continuity of care for patients registered at those facilities. But most of them are moving towards retention of health data for lifetime. Other facilities may prescribe different retention periods as per data type.

These facilities have an organizational policy in place, which covers guidelines of councils, accreditation compliance requirements or requirements by systems/HMIS, state or central compliance requirements, as notified by MoHFW for medical/health records.

While the total retention requirements under ABDM may propose a minimum retention period, for any health record there may be circumstances where records could be kept for longer periods for specific purposes and in some cases, there may be a provision for further extension upon special request.

A classification-based retention schedule may cover and minimize such scenarios, as duration for more valuable health data types could be mandated for longer periods.

4.2 Storage and Maintenance of Health Data Retention

ABDM stakeholders may be required to manage the technological infrastructure for collection and storage of core/master data through various centrally maintained registries. This may further improve quality of health data collection, storage, and dissemination with focus on consent based data sharing as key to building data architecture.

HIPs and HIUs may adopt feasible technology requirements including, cloud-based systems. Due to the need for exchange of health care data across platforms, compatibility across systems and platforms may be essential to seek alignment and compliance with interoperability standards.

Storage, transmission or any other aspect of processing of personal data is the responsibility of the data fiduciary and over-writing, anonymization or other method(s) of removal or erasure should be made possible on the request of a Data Principal.¹⁸ The same has also been mentioned in the HIU/HIP guidelines of ABDM per which any health records obtained by the HIU needs to be stored and managed securely in accordance with ABDM Health Data Management policy and Information Security Policy for external ecosystem.

4.2.1 Modes of Retention of Health Data

The method of storing patient information is one of the biggest data storage challenges organizations may face in integration of legacy systems while onboarding new systems into the health IT infrastructure. This indicates the importance of interoperability between different cloud vendors to facilitate smooth transition. An Electronic (E), Physical (P) or Original Form (O) of health data may be chosen as mode of retention by clinical establishments and health care providers although electronic medical records and electronic health records may be preferred.

With the possibility of hosting data off-premise, cloud data storage options seem to have gained popularity among healthcare organizations and storing health data in the cloud could give stakeholders better access.

To manage, store, and access health data, modern technologies, such as cloud, mobile, and new generation databases seem to have gained preference amongst users. A challenge that the healthcare domain would have faced in this regard pertain to security of healthcare data¹⁹.

¹⁸ [Health Data Management Policy, NDHM](#)

¹⁹ <https://archer-soft.com/blog/importance-healthcare-data-security>

With regards to the mode of retention of large imaging files, including those related to MRIs, etc., storage may be an issue of concern for smaller entities or clinics due to large format files. However, storage space availability may not be a challenge at large due to existing options of coding and storing large quantities of data, for example by some leading hospitals across India.

4.2.2 Maintenance and Exchange of Health Data

For scalability, flexibility, and economic reasons, cloud-based healthcare data sharing schemes have been proposed through data encryption and operation anonymization. However, users are hesitant to transferring private and sensitive data to cloud systems due to potential risks. In this regard, blockchain-based solutions have been widely discussed²⁰.

Legacy health IT systems may exchange resources internally and, as a result, may not be interoperable with external systems. This may negatively impact inter-organizational secure data access, which is often required, for example, during physician-specialist, physician-research organization interactions, etc. In this regard, newer approaches, for example, those combining blockchain, digest chain, and structured peer-to-peer (P2P) networking techniques may help resolve issues with legacy IT systems and data sharing agreements may also be defined.

For safeguarding retained data, the data fiduciary will have to ensure that in case of any outsourcing, the vendors must first be assessed to ensure they comply with the policy guidelines, to avoid any breach.

Any requests for extension of retention period or destruction before the recommended period shall be managed by the data fiduciary along with the data processor and they would be responsible for storage optimization techniques that provide high efficiency.

4.3 Data Classification for Health Data

Classification is the process of organizing data by relevant categories so that rules on usage, storage, retention, protection, and associated costs can be managed more efficiently. Data retention policies are essential for Personal Health Information (PHI) or Personally Identifiable Information (PII) due to the sensitive nature of these records, and retention being a resource-intensive procedure requires an understanding on what rules should apply to different categories of health data. These categories may be based on

²⁰ *Appl. Sci* (2019) 9, 1207; doi.10.3390/app9061207

the type of health records such as diagnosis, test results, discharge summaries or on the functionality of these health records.

While a more complex classification matrix may require strict governance, it shall essentially help in defining appropriate guidelines applicable for more sensitive type of data hosted on public platforms. Data can also be classified depending on its usage, the value and risk associated, content of documents, location, and time of access.

A classification-based retention schedule helps to:

- Automate compliance and systems
- Save costs in maintaining compliance
- Reduce risk of any privacy/security breaches for more sensitive type of data
- Discard less relevant or inactive records

4.2.1 Classification by Record Type

Across the globe, below types have been defined and they may have different retention periods to reduce risk of data breach as certain types of data are more valuable than others – hence, recognizing the value based on frequency of usage, and expected repeat references required for treatment or medical investigation, helps in classification.

1. OPD (Outpatient Department)

- General OPD
 - Patient exits hospital post-OPD consultation – **Records stored as General OPD Records.**
 - Patient is admitted to hospital post-OPD consultation – **Records to be stored as IPD Records.**
- Emergency
 - Any medical cases requiring immediate medical attention, including but not limited to accidents, burns, trauma, which are addressed under Day Care Unit – **Records stored as 'Day Care Unit Record' or 'Emergency Department Record'.**
 - Any medical cases requiring immediate medical attention, including but not limited to accidents, burns, trauma, bleeding, stroke, and subsequently leading to admission in the hospital – **Records stored as IPD Records.**
 - **Medicolegal cases** Patient is brought dead to the hospital – **Records stored as DeceasedPatients Records under Emergency Department**

2. IPD (In-patient Department)

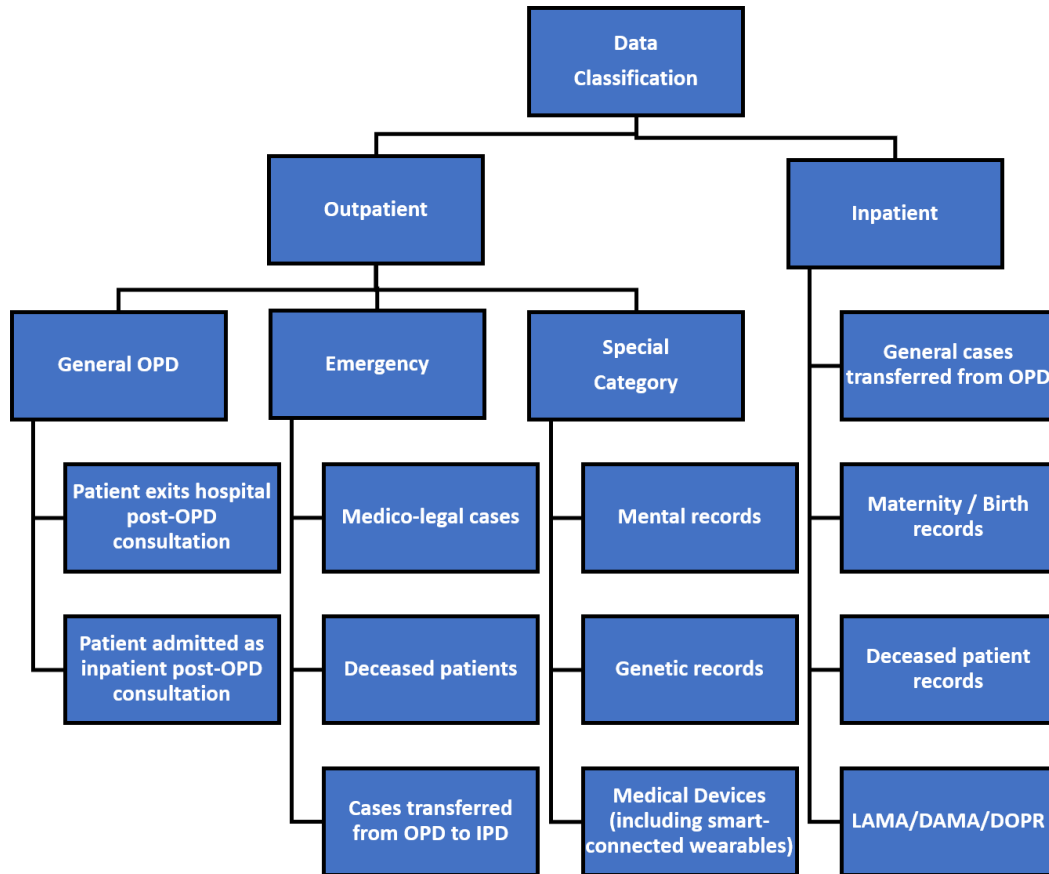
- General Cases transferred from OPD: Patients brought to emergency requiring admission would have their health data, generated at OPD, transferred to IPD for maintaining care continuum.
- Maternity/Birth Records: Birth- and maternity- indications will lead to generation of health data and retention.
- Deceased Patient Records: Incidences of death during or after treatment will lead to generation of health data and retention.
- Leave Against Medical Advice (LAMA)/Discharge Against Medical Advice (DAMA)/Discharge On Patient Request (DOPR) Records: Incidences of LAMA, DAMA, DOPR by admitted patients will lead to generation of health data and retention.

3. Special Category- (Can be part of both OPD and IPD)

- Mental records: Incidences of patients requiring psychological counselling or psychiatric treatment will lead to generation of health data and retention.
- Genetic records: Genetic records may be used for better disease prognosis and for improved clinical outcomes, leading to generation of health data and retention.
- Donor records: Donor records may be used for improved care delivery, leading to generation of health data and retention.
- Medical devices, including wearables and smart-connected devices: Use of medical devices for patient monitoring, or of wearables and smart-connected devices will lead to generation of health data and retention per guidance of “MDR 17 – Regulation of Medical Devices” of the Department of Pharmaceuticals, Government of India²¹.

²¹ <https://www.biotech.co.in/sites/default/files/2020-01/MDR17-%20Regulations.pdf>

Daily monitoring records of IPD patients may not fall under guidance of this policy.



4.2.2 Granular Data Classification

Levels of granularity may be attributed to the degree of data classification with or without identifiers. Accordingly, a high level of granularity is indicative of more detailed data classification as compared to low level of granularity.

The following matrix delves on granularity of data classification and its advantages and disadvantages, thereof:

Level of Granularity	Advantages	Disadvantages
Low	<ul style="list-style-type: none"> Minimize incidences of non-compliance with regulatory guidances 	<ul style="list-style-type: none"> May not adequately cover exceptionally new categories of patient cases

High	<ul style="list-style-type: none"> • May adequately cover exceptionally new categories of patient cases 	<ul style="list-style-type: none"> • May afford unreasonably greater bureaucracy over regulatory compliance.
-------------	--	---

4.4 Anonymization and Pseudonymization

Alternatives that are sometimes used instead of deletion are anonymization and pseudonymization. Pseudonymized data might still allow for some re-identification, while anonymous data cannot be re-identified. Because of the chance of re-identifying someone, the data retention period for pseudonymized data is no longer than the original data. Pseudonymization can be an alternative to keeping data for a longer period of time. However, the usability of this data is in most cases limited. No personal data is to be processed or stored in anonymized/pseudonymized form by any person/entity/Data Fiduciary except for any specific, clear, and lawful purpose and without informed consent of Data Principal. In addition, the scope and applicability of processing of personal data and sensitive personal data of children may follow clause 12 of Health Data Management policy. The process and method of anonymization/pseudonymization may be organization specific and may depend on Data Fiduciary, data processors, data sub processors, etc.

Anonymized / pseudonymized data may be deleted following fulfillment of the following conditions:

- a. If the Data Principal has made a request for data deletion.
- b. If the purpose for data anonymization/pseudonymization is achieved and there is no requirement further to store data.
- c. Data retention period has expired.
- d. If prescribed under any law prevalent at that point in time.
- e. As per any relevant court order.
- f. As per any government regulation or directive issued from time to time.
- g. For any other valid reason that those mentioned above.

Anonymized / pseudonymized data shall not be deleted even after there is a valid request of data deletion:

- a. If the data does not directly attribute to Data Principal.
- b. If the same is required for study of medical policies for benefit of society at large.
- c. If it is prescribed under any law prevalent at that point in time.
- d. As per any relevant court order.
- e. As per any government regulation or directive issued from time to time.
- f. For any other reasonable reason as notified by ABDM from time to time.

4.5 Country Comparison on Data Retention

Data retention policies of countries like Canada, United States, United Kingdom etc. vary. A single or a standardized retention schedule does not exist, and healthcare entities or health service providers in these countries have to follow both federal- and state-specific retention requirements, as well as rules applicable to them from other laws or acts.

Further, it was observed, that across countries compliance requirements may adopt some or all the below applicable mandates:

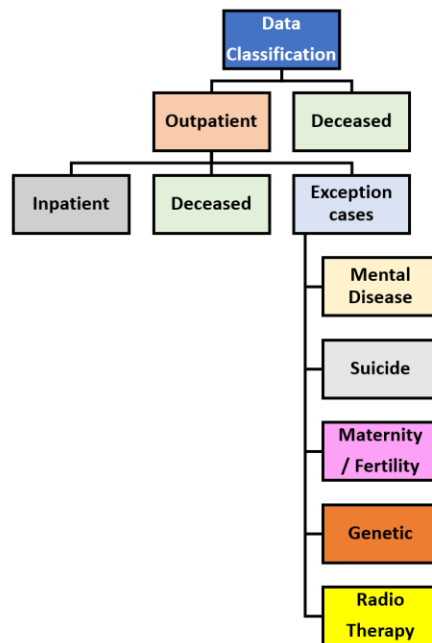
Country	Blanket Rules	State Mandate	Federal/National Mandate	Accreditation based Mandate	Other Guidelines	Links for Applicable Rules
Canada	✓		✓			Patient Record Retention
USA		✓	✓	✓	✓	State Medical Record Laws
UK			✓			Information Governance on Retention of Medical Records
Australia			✓			Health Sector (Clinical Records) Retention and Disposal Schedule
Iran			✓			Medical Records Retention in Iran
Korea			✓			Medical Service Act
Estonia			✓			
Thailand			✓			

The retention periods of various health record types are based on certain criterions, as mentioned here. For example, Canada and New Zealand have adopted a blanket structure for retention, and in Canada different states may have more granular classification additionally.

Other countries adopt a more granular approach for retention as discussed below:

- **USA (HIPAA)** - Covered Entities to retain medical records for 6 years, measured from the time the record was created, or when it was last in effect, whichever is later. Other regulatory frameworks of American Health Information Management Association (AHIMA), Code of Federal Regulations (CFR) etc. are also adopted.
- **UK (NHS)** is required to retain medical records for up to 20 years after the last interaction with the patient, up to 8 years after their death, or up to 25 years after the birth of the child for maternity records.

Referring to international data retention policies overseas, most record types are identified into the following categories:



- Inpatient
- Outpatient
- Deceased Patients
- Exception Cases which include – Mental Disease, Suicide, Maternity/Fertility, Genetic, Radiotherapy, etc.

A more detailed view across different health data type is presented in the below table:

Health Data Types	Canada ²²	USA ²³	UK ²⁴	Australia ²⁵
Inpatient	10 years from the date of last entry For Minors - 10 years from the time the patient would have reached the age of majority	10 years after the last discharge. Varies across states, ranging from 5 years after discharge to lifetime. For Minors- varies across states, ranging from 1 year after majority till the 30 th birthday	8 years from the date of last entry. In case of minor or adolescent, the records are maintained until 25 th or 26 th birthday after the end of their treatment	10 years from the date of last discharge. Different states may have different requirements Teaching Hospital - 15 years after the last discharge. For Minors - 15 years after the last visit or until the patient's 25 th birthday (whichever is later)
Outpatient	10 years from the date of last entry or, in the case of minors, 10 years from the time the patient would have reached the age of majority	Same as above ²⁶	Same as above	7 years after the last visit or until the 25 th Birthday, the longer one will be considered.
Deceased Patients		Most states do not practice distinct time retention for this type of records.	8 years after death	Up to 10 years after the Patient's death and may vary as per the state

²² [Standards of Practice – Patient Record Retention](#)

²³ [Medical Record Retention Periods – Medical Doctors & Hospitals](#)

²⁴ [INFORMATION GOVERNANCE Retention of Medical Records Policy, NHS Trust](#)

²⁵ [INFORMATION GOVERNANCE Retention of Medical Records Policy, NHS Trust](#)

²⁶ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3508852/>

Apart from the above major categories, some countries have below exceptions or additional categories which may be identified from the above classification as exceptions:

Health Data Types	Canada	USA	UK	Australia
Exceptions / Other Categorizations	7 years from the end of any clinical Research	-	Suicide Records - 10 Years	Rape Records 30 years
			Maternity/Fertility Records - 35 Years	Fertility records 35 Years
			Clinical trial - 15 years	Radiotherapy treatments 10 years after last discharge,
			Genetic Records - 30 Years	Diagnostic Records & Delivery Records Permanently
			On the advice of clinicians, data can be retained for a longer period if death has genetical relevance to the deed's family.	
			Obstetric records - 25 years	
			Donor records - 11 years	
			Oncology and Radiotherapy – 30 years	
			Mental Diseases Records 20 Years	

			Retention beyond last procedure for neurological, oncology records for 30 years	
--	--	--	---	--

A comparison of the above countries with India highlights how some of the types, such as "Outpatient" data maybe retained for longer duration. The table below provides a comparative perspective on the duration of health data storage in India vis-à-vis the global scenario.

Health Data Types	Reasoning	Lower limit of data retention across countries	Upper Limit of data retention across countries	India*
Inpatient	Longer retention period for critical medical records. Duration for Minors may be different and higher so as to account for birth related details up to the age of 30 years	5 years	30 years	10-15 years
Outpatient (including emergency)	Outpatient records are generally for short term ailments and do not require longer retentions	7 years	10 years	3-5 years
Deceased Patients	Only a few countries have guidelines for this type of record, especially in cases where a genetic implication may be applicable for the family	8 years	10 years	~3 years

Exceptions	All records pertaining to long term implications of medical conditions for patients	7 years	35 years	10 years ²⁷
-------------------	---	---------	----------	------------------------

**Facilities adopt applicable guidelines specified in section 2.2 of this paper or adopt an approach further specified in section 4.5.*

4.6 Use cases as per requirement of the health record in India

As observed across facilities in India, predominantly the purpose of longer-term data retention is to facilitate the below specific use cases:

- Insurance requirements as specified by IRDA
- Clinical trials
- Medico-legal cases where records maybe kept for up to 10 years or until the case has been closed²⁸

4.7 Existing Implementation of Guidelines for Retention of Health Records in India

As observed, Indian facilities comply to certain guidelines for retention as required by below guidelines. While state level or accreditation guidelines may exist, this is to highlight a few examples of how compliance is currently being enforced.

Council Mandated Implementation - Medical Council of India (National Medical Commission)

As per the **The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002²⁹**, below types of data have been identified:

- Indoor Records - standard proforma for 3 years from commencement of treatment
- Outpatient Records – 3 years
- Medico legal cases - until the final disposal of the case

Accreditation based implementation - NABL and NABH Accreditation

Records of reviews, including any significant changes, are required to be retained by accredited hospitals or laboratories. Records are also required to be retained of pertinent

²⁷ <https://main.mohfw.gov.in/sites/default/files/12%20Ch.%20XII%20Meical%20Record.pdf>

²⁸ <https://main.mohfw.gov.in/sites/default/files/12%20Ch.%20XII%20Meical%20Record.pdf>

²⁹ <https://wbconsumers.gov.in/writereaddata/ACT%20&%20RULES/Relevant%20Act%20&%20Rules/Code%20of%20Medical%20Ethics%20Regulations.pdf>

discussions with a patient relating to their requirements or the results of the laboratory activities.

Retention Periods for different data types have been defined for NABH/NABL are mentioned below:

- Inpatient Case Sheets – 7 years
- Outpatient Case Sheets – 5 years

All other records, summaries, (admission, discharge, or death), lab reports, pre analytical reports etc. are required to be retained for a minimum of 5 years.

4.8 Key Issues for Consultation

A data classification framework will be helpful in determining duration by the type of data. A more granular data with complex mechanisms, for ensuring compliance for retention, may require additional steps in validating the process of retention and maintenance, till expiration of retention period. Thus, addressing further questions as mentioned below, may help in identification of the right stakeholder for managing the overarching responsibility of data retention.

Further consultation on how retention schedules by data type may be considered for defining the policy on data retention is required and hence addressing below questions will be helpful:

1. Should a blanket retention duration be adopted for all health records in India or different schedules be defined as per a classification? Which is a better approach of retention?
2. How granular should data classification be? Is more granularity required beyond that presented in the sections above? Addressing this aspect of the Health Data Retention Policy would help assess whether minimalist data classification – pertaining only to inpatients and outpatients - would suffice the purpose of health data retention. A minimalist data classification would have both advantages and disadvantages. Please suggest your view in this regard.
3. How in your view will a detailed granular data classification enable a better health data retention? Please suggest your view on the classification of health record types as proposed above or if any further granularity is necessary and what are the overarching benefits for different stakeholders?
4. What should be the ideal duration for these different health data types?
5. While ABDM proposes that all entities opting to join NDHE must be able to retain health data in electronic format, and other entities of the healthcare ecosystem may consider physical or original formats, what options should be made allowable

as part of the policy being proposed? Health data records can be only digital, only physical, or combination in any hospital. Accordingly, the question arises whether all the above considerations should fall under one policy or under separate/independent policies?

6. Should there be a provision for extension of duration or retention of health data under the policy being proposed? What considerations should be made in defining the guidelines, allowing for such an extension?
7. Who shall have the apex authority to oversee and implement health data retention? Which entity as part of the ecosystem should be rolling out this policy at the macro-level?
8. How can smaller clinics or centres, both public and private, build capability in a timely and cost-efficient manner to take responsibility of data retention for long time periods?
9. How can business continuity be ensured in case of fall of the establishment, platform or service providers?

Chapter 5 - Proposed Approach for Health Data Retention Guideline/Policy

There is change in disease burden, from communicable diseases (CDs) to non-communicable diseases (NCDs), such as cardiovascular ailments, diabetes, and other metabolic syndromes. Interestingly, younger Indians are contracting these chronic metabolic syndromes at an alarming rate and a decade earlier than what their parents would have contracted 30 years ago³⁰. This shifting disease burden has prompted a growing trend among Indians in wellness and preventative medicine, early screening and rapid diagnoses, and care delivery. In such chronic NCDs, the first diagnosis may often lead to multiple engagements in due course for patients in earlier age groups. Thus, a longer-term retention will enable easy access to health records for further diagnosis, treatment, and monitoring for the patients.

Data can be stored permanently since the cost of retention is decreasing, and systems required for the same have capability for very long-term secure records management, including ease of exchange and real-time access. In this regard, the policy may leverage the available EHR Standards 2016, as notified by MoHFW. However, this may not be applicable for grassroots facilities in India and in cases where non-electronic formats are retained. These considerations establish the need for a more inclusive health data retention policy for India.

Determination of a stipulated period stems from the risk of leakage of sensitive personal data, and breach of data privacy. In order to minimize breach of data privacy, and for ease of capacity management by smaller facilities, guidelines on retention via policy will be helpful.

5.1 Proposed Classification

While a more granular classification could be considered, to simplify the process of classification and management of retention of records, the below structure shall fulfill a standardized approach for ABDM's recommendations for both Options 1 and 2, (as defined under section 3.1) of this consultation paper.

- Inpatient
- Out-Patient
- Deceased Patient
- Exception cases

³⁰ [https://www.who.int/data/gho/data/indicators/indicator-details/GHO/medical-doctors-\(per-10-000-population\)](https://www.who.int/data/gho/data/indicators/indicator-details/GHO/medical-doctors-(per-10-000-population))

5.2 Proposed Duration by Health Data Type

Based on the exploratory discussions in the above chapters, the retention schedule from the time of generation of the record by an HIP could be defined as per the below table for each type of health data.

Health Data Type	Minimum Retention Period
In-patient	10 years after the last entry/encounter. In case, of a minor patient, this type of record could be maintained until patient's 18th birthday or 10 years whichever is later
Out-patient	10 years after the last entry/encounter.
Deceased Patient	10 years after the last entry/encounter.
Exceptions, such as: <ul style="list-style-type: none"> • Medico Legal Documents • Immunization records • Clinical trials • Birth Register • Death Register 	Permanently

The guidelines applicable for the proposed policy beyond the retention schedule shall also consider mode or retention and governance of the data.

5.3 Mode of Health Data Retention

ABDM recommends that health data should necessarily be retained in electronic format, and the same shall be preferred for all entities opting-in to be a part of NDHE, such that health records are easy to retrieve as and when desired by a healthcare entity from interoperable systems.

If the policy is made applicable as per Option 1, as per section 3.1 of this document, the Electronic, Physical or Original Form of retention should also be acceptable for data retention. This would follow in the interest of clinical establishments and health care providers that may have decided to opt-out of ABDM.

5.4 Proposed Health Data Retention Governance Structure

The purpose of a data governance structure is to ensure that HIPs/HIUs and individuals trust the integrity of the retained data, which is essential for making patient care decisions such that legally allowable exceptions are accounted for. It should also ensure that the primary requirements as mentioned in section 2.3.2 of this document are always fulfilled.

The data governance structure for this policy can be defined similar to the governance structure in consonance with clause 6 of the Health Data Management Policy per which the appointed ABDM Data Protection Officer (DPO) shall be responsible for compliance related to data retention for all covered entities.

The DPO may additionally be responsible for matters concerning retention and building any audit mechanism, upwards from the grassroots levels, to avoid orphanisation of data in cases where an HIP/HIU no longer exists. Identified data fiduciaries under such a governance structure could be made responsible (as data custodian, for example) to ensure that data be retained in line with the guidelines throughout the life cycle of retention, as defined for a particular category of data.

ABDM would like to additionally emphasize that once the policy on data retention is released and made in effect, it shall not have an overriding effect on any of the existing laws or guidelines mentioned above or applicable. The superseding legislative guidelines as mandated should be followed by the healthcare ecosystem in compliance with total retention requirement.

5.5 Key Issues for Consultation

1. Will the governance model as per Health Data Management Policy be sufficient for the retention policy?
2. How will the policy regulation be enforced and what should be the structure across relevant entities responsible for retaining the health data?
3. How should the implementation of the policy be done in case the policy is made applicable for the ecosystem beyond ABDM?
4. Is there an alternative model or policy approach which could be considered?

Annexure

List of Questions

1. Whether there is a need for a Health Data Retention Policy and will Indian healthcare ecosystem benefit from such a Universal Data Retention Policy and what should be the key elements of this policy?
2. How should the guiding principle of this policy be determined for the benefit of stakeholders and ease of adoption by varying sizes of entities deciding to opt in for ABDM?
3. As per Option 1, it has been proposed that the policy would be applicable to all healthcare entities from health data retention perspective. As per Option 2, the policy will be applicable only to entities participating in ABDM? Which would be a better option for the scope of the health data retention policy?
4. How such a policy should be implemented given limitations in terms of infrastructure, capability, and sufficient understanding of health data in the healthcare ecosystem?
5. As ABDM has a provision for opt-out, in such a scenario what may be the possible implications from the perspective of health data retention?
6. Should a blanket retention duration be adopted for all health records in India or different schedules be defined as per a classification? Which is a better approach of retention?
7. How granular should data classification be? Is more granularity required beyond that presented in the sections above? Addressing this aspect of the Health Data Retention Policy would help assess whether minimalist data classification – pertaining only to inpatients and outpatients - would suffice the purpose of health data retention. A minimalist data classification would have both advantages and disadvantages. Please suggest your view in this regard.
8. How in your view will a detailed granular data classification enable a better health data retention? Please suggest your view on the classification of health record types as proposed above or if any further granularity is necessary and what are the overarching benefits for different stakeholders?
9. What should be the ideal duration for these different health data types?
10. While ABDM proposes that all entities opting to join NDHE must be able to retain health data in electronic format, and other entities of the healthcare ecosystem may consider physical or original formats, what options should be made allowable as part of the policy being proposed? Health data records can be only digital, only physical, or combination in any hospital. Accordingly, the question arises whether all the above considerations should fall under one policy or under separate/independent policies?

11. Should there be a provision for extension of duration or retention of health data under the policy being proposed? What considerations should be made in defining the guidelines, allowing for such an extension?
12. Who shall have the apex authority to oversee and implement health data retention? Which entity as part of the ecosystem should be rolling out this policy at the macro-level?
13. How can smaller clinics or centres, both public and private, build capability in a timely and cost-efficient manner to take responsibility of data retention for long time periods?
14. How can business continuity be ensured in case of fall of the establishment, platform or service providers?
15. Will the governance model as per Health Data Management Policy be sufficient for the retention policy?
16. How will the policy regulation be enforced and what should be the structure across relevant entities responsible for retaining the health data?
17. How should the implementation of the policy be done in case the policy is made applicable for the ecosystem beyond ABDM?
18. Is there an alternative model or policy approach which could be considered?

If there are any other issues that the public would like to be raised or comment on, they are invited and encouraged to do so.

Disclaimer

Please note that the above document is intended to be purely consultative in nature and is intended to provide an overview of the creation and operation of the Health Data Retention Policy. Nothing contained in this document should be considered legally binding in any manner. The NHA, its employees and advisors, make no representation or warranty and shall have no liability to any person, under any law, statute, rules or regulations or tort, principles of restitution for unjust enrichment or otherwise for any loss, damages, costs or expenses which may arise from or be incurred or suffered on account of anything contained in this document or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the document and any assessment, assumption, statement or information contained therein or deemed to form part of this document.