

Comments on Proposed Health Data Retention Policy Consultation Paper

Background

Consumer Unity & Trust Society (CUTS) expresses its gratitude to the National Health Authority (NHA), for inviting comments and suggestions on the Consultation Paper on the proposed Health Data Retention policy.¹

CUTS further congratulates National Health Authority (NHA) for proposing yet another policy to create a Health ecosystem along with National Health Policy, 2017, National Health Stack, and National Digital Health BluePrint. It is an important step towards empowering citizens and enhancing the health service industry. The strategic foresight on having a unified architecture on healthcare information and retention is a progressive step.

About CUTS International

CUTS international (CUTS) has come a long way from being a grassroots consumer-centric organisation based in Jaipur to opening overseas Resource Centres in Vietnam,² Africa,³ Switzerland,⁴ and the United States of America.⁵ It continues to remain an independent, nonpartisan, and non-profit economic policy thinks tank while opening various programme centres, namely: Centre for International Trade, Economics & Environment (CITEE)⁶; Centre for Consumer Action, Research & Training (CART)⁷; Centre for Human Development (CHD)⁸; and Centre for Competition, Investment & Economic Regulation (CCIER)⁹. It has been working toward enhancing the regulatory environment through evidence-based policy and governance-related interventions across various sectors and national boundaries. Further details about CUTS are available here.

Having conducted various studies and events, about Data Protection (such as Consumer Impact Assessment of Data Localisation, and Understanding the Impact of Data Localization on Digital Trade),¹⁰ Data Sharing,¹¹ and Encryption,¹² CUTS has observed a few critical issues in the draft architecture.

¹ Consultation Paper on Proposed Health Data Retention policy, available at [Consultation Paper on Proposed Health Data Retention Policy](#)

² [CUTS Hanoi Resource Centre](#)

³ [CUTS Africa](#)

⁴ [CUTS International, Geneva](#)

⁵ [CUTS WDC](#)

⁶ [CUTS CITEE](#)

⁷ [CUTS Cart](#)

⁸ [Cuts CHD](#)

⁹ [Cuts CCIER](#)

¹⁰ Objective: Understand and analyse the importance of digital exports for India's GDP and economy, along with the possible impact of data localisation barriers on Indian exports of digital goods and services.

Being a consumer-centric organisation, CUTS has observed a few critical issues in the consultation paper, which have the potential to impede consumer welfare, either directly or indirectly as a result of suboptimal clauses. In light of comments on Unified Health Interface (UHI)¹³ by CUTS, the current Health Data Retention Policy paper has been discussed in subsequent sections, along with a few recommendations and alternative model to address them.

The proposed Health Data Retention policy seems to be based on some broad principles that expressly or implicitly appear throughout the document. Key concerns about such principles are laid out below.

Health Ecosystem

National Health Data Retention Policy is visionary and could be a much-needed digital intervention in the Healthcare Ecosystem. It is a step towards the improvement of healthcare access in India, but the very objective and the meaning of the ‘ecosystem should be made clear first. What is meant by Health Ecosystem? For instance, if decision-making for public health concerns and research are the key objectives, the need and scope of policy need to be examined differently than a situation when the policy aims to address access and patient care-related challenges. Hence, therefore the policy orientation should be towards the identified goal and achieving such goals.

Consent

There are some issues that can be foreseen. These include Data Protection, Technological Challenges, and most importantly patient-physician trust. Let’s say, for instance, where a specialised or remote consultation is sought, it will be difficult for a new doctor or a new physician to obtain consent from the patient on their electronic health records. Here the more than consent building a Doctor-Patient trust is important. Further, once the health Data has been transferred what guarantee is it that it won’t be used for any other purpose than the purpose it has been consented for.

Expected Outcome: build a detailed and holistic understanding of the economic implications of existing and/or proposed data localisation barriers on India’s digital exports, while producing evidence to study alternatives to data localisation measures that are prohibitions to free data flow, to help policymakers in India and around the world to take an informed and appropriate and on data localisation.

<https://cutsccier.org/pdf/projectbrief-dtdl.pdf>

¹¹ [Examining the Rationale, Assumptions and Approaches to Non-Personal Data Sharing | ccier](#)

¹² [Understanding Consumers' Perspective on Encryption | ccier](#)

¹³ CUTS international Comments for National Health Authority on Unified Health Interface Consultation Paper, available at: <https://cuts-ccier.org/pdf/comments-on-the-consultation-paper-on-unified-health-interface.pdfvb>

Public Sector IT

Although the internet has reached masses and more than 80% of India's population has some level of internet access, the public sector IT system lacks robust websites, internet speed, and a seamless user experience is mostly lagging. This is not quite the case for most public sector websites at the moment. A reference is largely coming from the experience during COVID vaccine registration at Cowin.¹⁴ Now, imagine thousands of people trying to consent and share data on such an interface along with understanding the nature of the consent. Given that country's digital illiteracy rate are high, interfaces and retentions need to be kept simple and user-friendly. A heavy reliance will be placed on Doctors or Physicians, let's say at rural areas that are local to them, for digital facilitation, might even make them trust blatantly on Data sharing and consenting.

Stakeholders Training

The treating entity should be well trained whilst dealing with patients' personal data. It is important for stakeholders to realise that the procedure of data sharing is consent-based and not influence-based.

Supplementary data

It is true that with prior health records, a doctor or physician can flag the severity of diseases. Let's say for someone who has a history of high blood pressure or diabetes could be more prone to COVID-19, or obesity could be one of the other factors. Unknown risks could be identified with the availability of the medical history, and disease endpoint data, this would require that the health data be supplemented with other additional details such a lifestyle. This might be a good opportunity for the insurance companies and other interested entities to hog the lifestyle data; it might not be as realistic for the Patients.

No regulatory framework in place

Ameera Shah, Managing Director, Metropolis healthcare Limited said, *“Digital health was at a nascent stage and Covid-19 pushed it forward. There has been a transformational leap in the way healthcare potentially operates from the pre-covid era to post covid era. While on one hand, you have digital healthcare companies trying to aggregate demand while on the supply side things are highly fragmented. While we know that 70 % of decisions are based on diagnostics, there are an **estimated 1.50 lakhs labs in the country with no regulatory framework in place**. Since there is no registration methodology one is given to understand that there is no governance framework within the country which could put minimum standards for effective regulation of labs. This has led to the proliferation and mushrooming of labs which has increased accessibility but has reduced quality.”* The fact that the entities

¹⁴ <https://www.cowin.gov.in/>

are themselves not regulated and there plausibly remains no effective means to regulate them. Effective registration regulation should be the prime the concern of the regulatory authority.

Recording Date

Further the Data could be recorded either in physical form, electronic form, or even a hybrid form. A combination of both - physical or electronic data- should be followed. Further, one single policy should be followed for the considerations above.

Use of security mechanisms to steer data retention

In a healthcare organization that handles peoples' data, there will be certain employees who will break the rules whether intentionally or by accident. The chances of this happening can be reduced by using security policies to help prevent the mishandling of data. For instance, in case an organization has a policy requiring the employees to save patient data to a specific encrypted server volume where the data is secured and backed up. In that type of situation, you would not want employees to save patient data to the hard drives on their PCs. To ensure this, security policies can be put in place to block users from saving data to local hard drives, and instead use server backup services where data is encrypted and sent to secure offsite locations.

WHO formulation of five basic problems in the health information - Must be considered while considering formulation of the policies.

- The information available was irrelevant,
- The quality of the data was still poor,
- Duplication and non-uniformity,
- Delays in reporting & feedback, and
- Suboptimal use of information.

Penalties and compensation for non-compliance

The draft policy fails to explicitly mention the penalties and compensations for non-compliance with the policy. Now if the entity fails to record the data, or retain the data in a particular format, or decides several times to opt-in or opt-out of the policy, there are no consequences for the same. It is recommended that there should be some level of penalty or compensation for non-compliance applicable to the entities.

The guidelines severally lack a grievance redressal policy for breach of any regulations that will authorise entities to Create, Utilize, Maintain (retain), and distribute the Health data of the patients.

There is no accountability on hospitals

Hospitals should be held accountable for any data mismanagement under the retention policy framework. It is recommended that the scope of the policy must also encompass accountability on hospitals and other entities which store health data.

Risk of Exclusion

The policy must ensure that benefits are delivered to the right consumers of the policy that is the patients and people reaping the health benefits.

Please refer to the list of Questions (Draft Health Data Retention consultation paper).¹⁵

Question 1: Whether there is a need for a Health Data Retention Policy and will the Indian healthcare ecosystem benefit from such a Universal Data Retention Policy and what should be the key elements of this policy?

- Yes, there is a need for a Health data Retention policy to create a health Ecosystem.

Recommendations

The purpose and aim of the formulation of a health data retention policy are to create an ecosystem in health, within India. The Health Data Retention Policy is a step towards the Ayushman Bharat Digital Mission (ABDM) which is aimed to develop a necessary support system for integrated digital health infrastructure in the country. It will bridge the existing gap among different health stakeholders in the ecosystem through digital highways.

As per WHO Global strategy on digital health 2020-2025 (hereinafter referred to as ‘WHO guidelines’), the need of the hour is to build a healthy ecosystem, a Health Data Retention Policy. Under ABDM, it is important for all the stakeholders to benefit from the ecosystem and, among several other policies; Health Data retention becomes one crucial policy that requires a strategic implementation. The foremost step is to bring forth such a policy.

One Policy for All

Whilst the Consultation paper on Health Data Retention policy only covers the retention aspect of it, the draft should be mindful of all four factors of a health ecosystem – *create, utilise and maintain (retain), and destruct health data*. What we need is a policy enclosing all; one policy for all. It will be difficult to refer to numerous documents and laws simultaneously while dealing with health data. More importantly, there needs to be consistency and coherence between different policies or different components of a policy. It

¹⁵ Consultation paper on proposed health data retention Policy, Annexure - pg. 42, available at: https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation_Paper_on_Health_Data_Retention_Policy_21.pdf

will further allow easy access and source of reference for consumers of the policy. Retention is only one of the building blocks for the ecosystem.

The life cycle of records management begins when information is created and ends when the information is destroyed. The creation of information is easy to establish. Thereby, most entities do not face concerns whilst creating or using information. Although in a country like India, where most of the information creation happens through handwritten prescriptions or Diary records, the capabilities of doctors/hospitals to create a digital record and engage in the digital entry is important. Data retention means nothing without adequate infrastructure and healthcare facilities. It is also the process step of maintaining information, which causes issues to arise. The figure below (*Fig. 1*)¹⁶ provides a simple reflection of the entire records retention process as recommended.

Patient: The goal should be to manage each step in the record life cycle to ensure record availability. It is also pivotal to understand the role of challenges that patients face and their ability to correct, edit, and retrieve their own health Data.

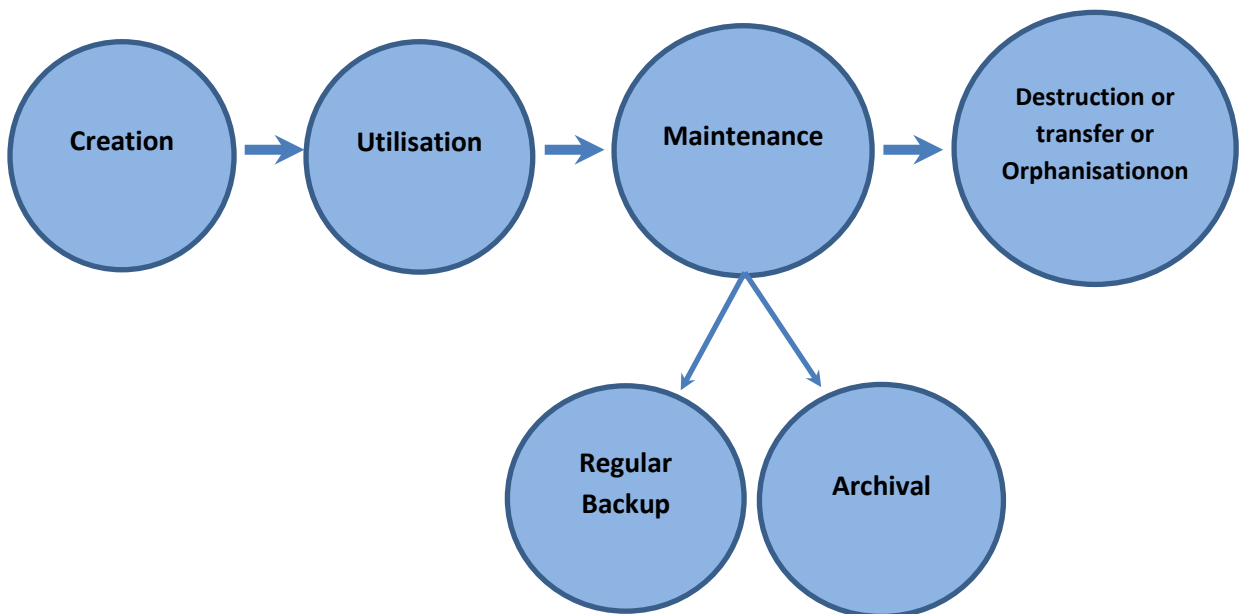


Fig. 1

¹⁶ [Retention and Destruction of Health Information](#)

Key elements of the Policy

Apart from other key ingredients in the policy, the following should be the guiding factor in policymaking for Health Data Retention Policies. By taking time to create an effective medical retention policy, one reduces the risk for non-compliance with the health Data retention law and secures protected health information, for easy access in case of inquiries from the stakeholders, inclusive of and not limited to patients, researchers, etc. At a minimum, the policy should highlight and ensure that the health information **policy is patient centric**. That the information is available keeping in view of what it has been consented for. Staff Training should be for Health Data records retention and access is necessary.

Question 2: As per Option 1, it has been proposed that the policy would apply to all healthcare entities from a health data retention perspective. As per Option 2, the policy will apply only to entities participating in ABDM? Which would be a better option for the scope of the health data retention policy?

Question 3: How such a policy should be implemented given limitations in terms of infrastructure, capability, and sufficient understanding of health data in the healthcare ecosystem?

- An 'Opt-in' policy should be followed under option 2 for a pilot phase. Moving to an 'opt-in' approach for option 1, with express incentives along with generating awareness, capacity, and infrastructure for stakeholders to join the ecosystem. The Pilot will allow understanding of the issues at hand, which can further be dealt with for other stakeholders for better compliance.

Recommendation

The kind of infrastructure that the National Digital Health Ecosystem (NDHE) assumes to be already in place may prove to be a restriction. The nature of the data to be collected requires physical infrastructure as well as human resources earmarked for health information management. Given the fund-starved nature of India's health system, this is going to be the single biggest challenge for any effort at digitization of health records.

While considering the implementation and limitations in terms of infrastructure capability, a sufficient understanding of Health Data in the health care system could be developed through a Pilot mission (One Year). Retention of Health Data policy is one of the key ingredients of achieving an ecosystem in health. Further to ensure that India is ready for an ecosystem like this, as its dependence on Data privacy and several other factors that help in strengthening the system, the need of the hour is a strong framework on the deciding and elevating factors in the policy.

A pilot mission will help build, strengthen factors such as Data storage, Data privacy, consent, infrastructure and sufficient, understanding of the health data nation, etc. The policy,

can briefly through its pilot mission prepare itself for *Atmanirbhar Bharat* days ahead. Learnings from the pilot mission can help understand the advantages and disadvantages of the retention policy and simultaneously efficiently roll out option 1 after a year's pilot. 'Opt-in' scope for entities in Option-1. The option allows for a uniform approach towards health data retention enabling ease of adoption of any future policy/guidelines, reducing friction in any cases in data retention. Adherence by each entity might not be difficult as posed a challenge in the consultation paper, as entities are now opting in rather opting out of a policy under option 1.

Express Incentives

Express Incentives must be provided to facilitate easy opt-in responses for all the stakeholders and entities. This may include reduction in the cost of compliance, complimentary training for strengthening policies, Data storage, Data maintenance, and simultaneous destruction, etc.

The policy post-pilot period must be applied to the entire healthcare ecosystem, requiring the necessary capability, training, and suitable technologies to be implemented by all stakeholders. The policy should granularly, adopt a citizen-first approach while implementing various parts of the National Digital Health Ecosystem (NDHE), given the highly sensitive nature of the health data of data principals that will be shared with Health Information Providers (HIPs) and Health Information Users (HIUs). While the HDMP does elaborate on the rights of digital principals—such as the right to confirmation and access,—it does not make adequate provisions in case of disputes with data fiduciaries and the right to correction and erasure of Health data.

Question 4: Should blanket retention duration be adopted for all health records in India or different schedules are defined as per a classification? Which is a better approach to retention?

- Different schedules should be defined for health data retention as per the classification instead of one blanket retention policy.

Recommendation

Active and Inactive Records¹⁷

A better approach for retention could be to keep records on an Active and Inactive record basis. This would mean for the records which are consulted or used on a routine basis should be separated from the records which become inactive due to their minimal usage.

Routine functions may include activities such as the release of information requests, revenue integrity audits, or quality reviews. Inactive records could include records that are rarely used. Inactive records usually involve data of a patient who has not sought treatment for some

¹⁷ <https://library.ahima.org/PB/RetentionDestruction#.YcWYcslByM>

time or one who completed his or her course of treatment. Defining active and inactive records also may depend on other issues such as physical file space, the amount of research done, and the availability of off-site storage. For example, because of limited file space, an organization may determine that records are active for one year from the discharge date. After one year, the record is moved to off-site storage or scanned to a DVD and considered inactive. In this instance, being inactive does not mean that the record can be destroyed because the record has not yet met its full retention requirement. Each organization should determine a cut-off point (usually a discharge date) that signals the time at which a record becomes inactive. The policy may consider the activeness of data based on total retention periods as prescribed or accessing of records etc. Identifying and maintaining active and inactive records is an important step in the successful maintenance of a filing system.

The first step in establishing a data retention plan is to figure out what type of data might potentially need to be retained. In healthcare organizations this typically includes Electronic health records, E-mail messages, pictures, and communications, etc. Depending upon the nature of the healthcare organization there may be other types of data that need to be retained.

Granular retention of data is not recommended for small entities or small clinics as it might increase the cost of compliance, thereby increasing the retention cost. Rather a two form approach could be identified, where segregation is based on entities (one way to do it is to create slabs on tax bases) and highlighting the mandatory sections in the data Retention form for smaller entities as against the entire form for bigger entities. The bigger organisations, let's suppose have a more granular form of retention given the length of cases it receives on daily basis.

Question 5 - How in your view will a detailed granular data classification enable 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?

- The current form of classification as suggested in the consultation paper with a little tweak for a steady alignment to International standards involving **Outpatient** and **Inpatient**, along with **Special category**, **Emergency**, and **Exceptional Cases**, is an adequate form of Data Collection.

Recommendation

The identification of such classifications is neither too granular nor something a small entity might not be able to maintain. Depending on the entity, easy classification of outpatient and inpatient data can be maintained, along with several other factors such as mental disease, suicide, maternity/fertility which could be maintained under exceptional cases.

Direct identification of an Adult and a Minor is highly recommended, wherein a Nominee or Guardian should also be appointed for both Adult and Minor's health data respectively. This should be highlighted not only for data retention but also for data destruction, storage, and other means in the ecosystem of data retention.

A Nominee

A nominee must be appointed for the sole purpose of having someone else other than the owners of the data have access to the Health Data. This is to cater to the circumstances, wherein the first owner of the Data becomes incapable of consenting to the usage of the data due to several factors.

Should the Data be available to any nominee appointed by the owner of the Data? Given the need to appoint a nominee as highlighted above, if allowed and agreed upon in the policies, what should be the guiding factors?

A guardian

In the case of a Minor's Data, a guardian should be appointed to seek consent on behalf of the minor (owner of the Data), who is legally incompetent to consent.

A third narrow classification should be done keeping in mind the research for development in the health ecosystem. It is recommended that the classification should be done based on Deadly or ill-researched Diseases, a list recommended by NHA. This will help in the promotion of research, development, and innovation in the Health, Pharmaceutical, and Health-tech industry.

Employee Training - One of the most critical aspects of complying with data retention requirements is that of employee training. Employees in healthcare entities need to be trained in properly and efficiently handling data. From a legal perspective, it is beneficial to implement a formalized program to educate employees on data retention and other aspects of policy. Each employee's participation in this program should be documented, and the employee should be required to sign a statement indicating that they have been through the training program and understand the requirements for data handling. The policy recommendation fails to employ an employee training programme for entities opting in for Health Data Retention Policy. Their incentives should be linked to their performance.

Recommended practise timeline in India¹⁸

Health Data Type	India
Inpatient	Adult - 10 years after the last date of entry. Minor- 15 years after the last visit or until the patient's 25 th birthday (whichever is later).
Outpatient (Including Emergency)	Adult- 5 years after the last date of entry. Minor-5 years from the time patient would have reached the age of majority.
Deceased patient	8 years after Death
Other Categorizations	10 years ¹⁹
Exceptions such as <ul style="list-style-type: none"> • Clinical Trial Records • Research Records • Death Register • Birth Register • Medico-Legal Documents • Immunization Records 	Permanently

Destruction of Patient Health Information²⁰

Destruction of patient health information by an entity or provider must be carried out following the law pursuant to a comprehensive written retention schedule and destruction policy. Records involved in any open investigation, audit, or litigation must not be destroyed until the matter has been closed. It is recommended that patients must be notified before any information is eligible for destruction. Upon the request of the patient or the nominee, the health data that has been retained must be made available for personal retention by the patient or otherwise be destroyed by creating an abstract of the destroyed information. Organisations must ensure that paper and electronic records are destroyed with a method that provides for no possibility of reconstruction of information. A statement of destruction must be recorded, accompanied by the used method of destruction. It must also include:²¹

- the time that will elapse between acquisition and destruction or disposal,
- safeguards against breaches,

¹⁸ Consultation paper on Health Data Retention policy, chapter 4, page 35-36.

¹⁹ <https://main.mohfw.gov.in/sites/default/files/12%20Ch.%20XII%20Meical%20Record.pdf>

²⁰ Under the HIPAA privacy rule (45 CFR, Parts 160 and 164).

²¹ Under the HIPAA privacy rule (45 CFR, Parts 160 and 164), when destruction services are outsourced to a business associate the contract must provide that the business associate will establish the permitted and required uses and disclosures and include the elements stated above.

- Indemnification for the organization or provide for loss due to unauthorized disclosure.

Other Questions: Among others, few of the propositions to be noted before the Policy formulation.

1. Should an entity be requesting for a nominal cost while allowing access to the health data or should the Data be made available for free of cost?

- If the charges are levied this could help an entity in reducing its cost of compliance subsequent to the Health Data retention policy, making it further nominal for entities to retain the Data. But if the fees is levied it might end up adding another set of cost to the entities. A further clarity on this is needed.

2. What should be the minimum time frame for the recording of the Data under the health Data retention policy?

- Whilst it is understood, that health data must be digitally recorded, there would be times when smaller clinics or other entities might initially end up recording manually and later update the health data digitally as per the policy. It is pertinent to guide the entities on the minimum time frame in which the data must be recorded digitally as per the Health Retention Guidelines.

Conclusion

CUTS International looks forward to National Health Authority accepting the suggestions given above, and assisting NHA in its endeavours of empowering consumers and individuals. For any clarifications/further details, please feel free to contact Tanya Goyal (tng@cuts.org).