Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE MUMBAI BKC NEW DELHI MUNICH NEW YORK

93 B, Mittal Court, Nariman Point, Mumbai 400 021, India
tel +91 22 6669 5000, fax +91 22 6669 5001

www.nishithdesai.com

COMMENTS ON CONSULATION PAPER ON PROPOSED HEALTH DATA RETENTION POLICY, 2021

Nishith Desai Associates — **National Health Authority, India**

December 24, 2021

December 24, 2021

To,
National Health Authority,
9th Floor, Tower - 1 Jeevan Bharati Building,
Connaught Place,
New Delhi - 110001

Re: Comments on Consultation Paper on Proposed Health Data Retention Policy

We thank the National Health Authority for seeking feedback on the Consultation Paper on Proposed Health Data Retention Policy released on the November 23, 2021 ("**Consultation Paper**").

We appreciate the approach taken by the National Health Authority for laying down a framework for health data retention for the Ayushman Bharat Digital Mission ("**ABDM**") architecture, and considering its extension to the entire healthcare system. The implementation the Health Data Retention Policy would create uniform principles for the retention, use, storage and accessibility of health data in line with international best practices across all healthcare providers including hospitals, laboratories, pharmacies, healthcare professionals, insurers, health tech companies etc. who collect health data (collectively known as "**healthcare establishments**").

At Nishith Desai Associates we take a keen interest in contributing to regulatory engagements. We are a research-based law firm and enjoy high credibility in respect of our independent research and assist number of ministries in their policy and regulatory work. Over the years, the Pharmaceutical, Healthcare and Medical Device Team at Nishith Desai Associates has contributed the healthcare policy of India, and has also represented various Pharma, healthcare, med-tech and medical device companies on regulatory issues and represented them in various deals in PE and VC investment, M&A, Joint Ventures etc. Our Healthcare Practice has been ranked as a Band 1 practice for life sciences by Chambers and Partners for five consecutive years. We have also been recognized by Asialaw and India Business Law Journal.

Building upon our interest in participating in regulatory work, we have provided our detailed comments below based on the questions raised in the Consultation Paper. We hope this aids the National Health Authority in determining the approach to health data retention in India.

We look forward to engaging further.

Nishith Desai Associates Team.

COMMENTS ON CONSULTATION PAPER

In this section, we have provided responses to the questions posed in the Consultation Paper on the scope and implementation of the proposed health data retention policy.

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?*

NDA Comment: Yes, there is a need for a Health Data Retention Policy. The Indian data protection framework- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Data Protection Rules**") issued under the Information Technology Act, 2000 (collectively "**current law**") does not provide for retention of data. While the Draft Data Protection Bill, 2021 (contained in Report of the Joint Parliamentary Committee on Personal Data Protection Bill) ("**DPB**") does require data retention of personal data including health data. However, it does not specifically address the context of retention of health data, use of retained health data, manner of storage etc. A specific Health Data Retention Policy would lay down the scope, elements and the governance approach and maximisation of benefits from the use of the retained health data. This would also ensure uniformity in the approach to governance of health data across the healthcare system.

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?*

NDA Comment: The guiding principles for the policy should focus on enabling interoperability and ease of exchange and access of health data of individuals. Since, health data is sensitive in nature and also strategic to the nation; access to health data should be on a 'need basis'. Since the proposed policy will enable retention of data for a long period of time, it must ensure a balance between the security and access/use of health data. Further, the proposed policy should also provide for the subsequent uses (commercial and non-commercial) of retained health data.

For ease of adoption of the policy, stakeholders (including all varying sizes of entities) must have in place basic infrastructure to ensure compliance with reasonable security practices and other basic tenets of data protection laws. We suggest that the policy should not be granulated in terms of the technical requirements and instead impose obligations required to be adopted by stakeholders in their capacity.

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?*

NDA Comment: From a long run perspective, adoption of Option 1 would enable uniformity across the industry. This would be in line with the object of interoperability of health data which the ABDM seeks to achieve. However, enforcement of Option 1 would be a lengthier process and burdensome. Therefore, in our opinion, at the present, Option 2 is a viable approach and will enable faster execution of the prospective policy. We recommend the consideration of Option 1 after substantial progress has been made with the implementation of the prospective policy within the ABDM ecosystem.

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?*

NDA Comment: The policy should be implemented in a phase-wise manner to ensure compliance and adoption of the policy by all stakeholders. While we understand that not all stakeholders may adopt the policy voluntarily, we suggest implementation of the policy in the following phases:

(a) Phase I: Voluntary period of compliance for all healthcare establishments during which time an exemption from compliance with the policy is provided;

(b) Phase II: Mandatory period for compliance for participating entities;

(c) Phase III: Policy will become binding and compliance with it will be mandatory for all healthcare establishments handling health data.

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?*

NDA Comment: We understand that if the prospective policy is intended for only participating entities, then entities opting out of the ABDM will not be required to continue compliance with the prospective policy. We recommend that the prospective policy include a provision extending applicability of data retention obligations to entities opting out of ABDM. This would ensure a standardized approach and enable faster transition towards a unified data retention policy across the healthcare system.

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?*

NDA Comment: Yes, in our opinion a blanket retention duration would ease the burden of compliance and enforcement of the prospective policy. To this end, the prospective policy need not include provisions classifying types of record. Instead, the Health Data Retention Policy should be made universally applicable to every record of health data irrespective of

purpose of collection, context of collection of health data and establishment collecting health data. However, entities collecting health data for a limited purpose may be exempted from this requirement and the prospective policy may define the conditions of such exemption and prescribe a shorter duration for retention for such purposes.

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.***

NDA Comment: The current law[1] and the DPB[2] treat all forms of health data as a single category of data. Given this uniform approach to regulation of the collection, processing and storage of health data under the general law, a granular classification for the purpose of health data retention would complicate compliance and enforcement.

We understand that the object of ABDM is to create an integrated health information architecture. ABDM contains a wide range of stakeholders including health technology companies and insurers who do not necessarily maintain health records in the form of inpatient and outpatient records. Therefore, a minimalist approach to health data classification will enable wider applicability of the proposed policy.

Hence, adopting a broad approach to health data records classification, we recommend that the prospective policy categorize health data records basis the legality of the data subject- (i) adult patient records; and (ii) minor patient records.

We recognise that adoption of a minimalist classification would mean that entities collecting health data for limited purposes will also fall within the ambit. Therefore, to mitigate this, exemptions may be provided from retention obligations to certain types of purposes of collection of health data such as for employment records, anonymised data for research purposes etc. which are not necessarily for the purpose of rendering healthcare.

[1] Health data, medical records, genetic data and biometrics are sensitive personal data or information under the Data Protection Rules.

[2] Health data means "*the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associated with the data principal to the provision of specific health services.*" Health data is classified as sensitive personal data.

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?*

NDA Comment: As contained in our response to question 7, we suggest a broad classification to create a wider scope for health data retention obligations. To this end, we recommend the classification of health records into (i) adult patient records; and (ii) minor patient records.

From an impact perspective, the prospective policy is less likely to clash with the applicable general data protection laws if a broad-based classification is adopted. While from an enforcement perspective, this bring all entities collecting health data (irrespective of the nature of record) into its ambit, therefore ensuring wider applicability of the data retention policy.

9. *What should be the ideal duration for these different health data types?*

NDA Comment: We suggest from precedents set forth in other jurisdictions that the stakeholder must ensure patient records are retained and accessible for a minimum of:

(i) ten years from the date of last record entry for an adult patient;

(ii) ten years after the date of last record entry for a minor patient, or two years after the patient reaches the age of eighteen, whichever is longer.

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?*

NDA Comment: We agree with the proposed view of mandating retention of health data in electronic format for participating entities in National Digital Health Ecosystem ("**NDHE**").

Should the proposed policy be extended universally to all entities in the healthcare ecosystem, then a phase-wise manner of implementation may be considered (as detailed in our response to question 4 above). A period of voluntary compliance with the requirement of electronic health records may be provided. During this period, non-participating entities may maintain health records in digital, physical, or combination formats. Post the expiry of such voluntary period, we propose that digital storage of health records become binding on all entities. A single policy may govern all types of health data records (digital, physical, combination) for the ease of compliance.

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?*

NDA Comment: Yes, there should be a provision for extension of duration or retention of health data for specific purposes and in some cases upon request by the stakeholder. We have suggested the period of retention in our response to question 9 above. The stakeholders should be provided with an option to retain the data for a longer period upon obtaining consent from the data principal subject to periodic reviews.

The extension of the retention period may be allowed under certain grounds which may include:

(i) Research purposes by taking consent of the data principal;

(ii) For patient treatment purposes on request of a health care practitioner;

(iii) Where the health record is the subject or presented as evidence in an ongoing litigation.

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?*

NDA Comment: We understand that the Health Data Management Policy, 2020 ("**HDMP**") – the policy which governs data protection and information security under ABDM - requires the National Health Authority to adopt guidelines on health data retention. The HDMP is administered by a Data Protection Officer, a government officer who overlooks the data practices of the data fiduciary. Therefore, we suggest that the Data Protection Officer under the HDMP oversee and implement the proposed policy as well.

In the event the data is sought to be implemented at a macro level, we suggest that the health data retention policy be issued by the Data Protection Authority proposed under the DPB. If the Policy is to be issued under the current law, then it may be issued by the Ministry of Electronics and Information Technology, Government of India which is the nodal ministry for the enforcement of the current law in India.

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?*

NDA Comment: Smaller healthcare establishments may outsource their data storage. To this effect, the policy may define controls to be implemented in health data outsourcing to ensure security of the data, migration of data, and disaster and back-up recovery plans. The Consultation Paper suggests deploying cloud-based software for the storage of health data. Smaller healthcare establishments may consider availing the services of cloud services providers for fulfilling the data retention obligations.

In addition to this, we also suggest the adoption of efficient data management practices at an organizational level:

(i) Only data necessary for the purpose of providing the healthcare service must be collected;

(ii) Mechanisms for removal of redundant data before storage;

(iii) Standardised formats for recording data collected;

(iv) Create an inventory of data and providing limited access to retained data.

14. How can business continuity be ensured in case of fall of the establishment, platform or service providers?

NDA Comment: The policy must place the responsibility of health data retention on the healthcare establishment. In doing so, the proposed policy must specifically state that the healthcare establishment shall develop and establish a robust framework for maintaining records of data and testing business continuity and recovery procedures arising out of any adverse events.

To mitigate risks arising out of outsourced data storage services, the healthcare establishment shall be required to maintain adequate control over the health data records and shall have the right to intervene with appropriate measures for its business continuity.

In instances where the healthcare establishment itself ceases operations; the proposed policy must provide for alternate measures. To this end, we propose that the proposed policy envisage the creation of national repository of health data which may store (i) critical health data necessary for public interest and; (ii) health records which are required to be stored for a prescribed period by a healthcare establishment which ceases to exist during the pendency of retention period.

15. Will the governance model as per Health Data Management Policy be sufficient for the retention policy?

NDA Comment: We understand that under the HDMP the ABDM-Data Protection Officer overlooks data protection and compliance. At the organizational level, a grievance officer is responsible for addressing grievances of data subjects. The HDMP does not provide specific details of the governance structure and instead states that it will be informed from time to time. Till date, there are no further policies or clarifications have been issued with respect to the governance structure. Therefore, due to the rudimentary structure of governance under the HDMP, we believe that it is not adequate.

The HDMP also fails to provide details regarding the size, composition, selection process, tenure, powers, functions, terms of removal, financing and the accountability framework of the authorities sought to created under the ABDM. Further, the HDMP does not address

whether the ABDM governance mechanism will be integrated with the Data Protection Authority proposed under the DPB.

We suggest that HDMP and proposed data retention policy broaden the scope of the duties of the grievance officer at the organizational level to extend the responsibility to overlook the healthcare establishment's data practices. While, the government-appointed Data Protection Officer may be assigned certain healthcare establishments for the purpose of ensuring enforcement of the policy. The Data Protection Officer will be required to coordinate between the grievance officers of the data fiduciary and the regulator, overlook the data retention mechanisms, escalate non-compliance to the regulator etc. Once the DPB is enacted, this governance structure may be integrated with the mechanism of the Data Protection Authority proposed thereunder.

16. *How will the policy regulation be enforced and what should be the structure across relevant entities responsible for retaining the health data?*

NDA Comment: The proposed policy may be enforced in the same manner as the HDMP. We have suggested a three-tier mechanism in our responses to question 15 above. If the proposed policy is sought to be implemented universally across the healthcare system, then non-NDHE entities must be provided with a voluntary period for compliance before the policy is mandatorily enforced (discussed in detail in response to question 4).

17. *How should the implementation of the policy be done in case the policy is made applicable for the ecosystem beyond ABDM?*

NDA Comment: Our responses to questions 4 and 10 above detail our suggestions on the implementation of the proposed policy. Basis our understanding of the scheme of the Health Data Retention Policy advanced in the Consultation Paper, we suggest that phase-wise approach with a voluntary compliance period must be adopted should the proposed policy be made applicable universally.

18. *Is there an alternative model or policy approach which could be considered?*

NDA Comment: We suggest that the proposed policy should restrict its scope to (i) prescribing the retention period for the health data; (ii) exemptions from retention obligations; and (iii) management of retained health data. The privacy aspects and data protection obligations pertaining to security, consent, processing etc. should be governed under the applicable data protection laws. Further, the enforcement of the policy may be continued as under the governance structure of the HDMP. We suggest that this governance mechanism be clarified and aligned with the applicable data protection laws.