The Centre for Internet and Society's comments and recommendations to the:

National Digital Health Mission: Health Data Management Policy

Date 21st September 2020

By **Shweta Mohandas, Pallavi Bedi, Shweta Reddy,and Saumyaa Naidu**

Edited by: **Ambika Tandon**

The Centre for Internet and Society, India

Introduction

The Centre for Internet and Society (CIS) is a non-profit research organisation that works on policy issues relating to privacy, freedom of expression, accessibility for persons with diverse abilities, access to knowledge, intellectual property rights and openness. It engages in academic research to explore and affect the shape and form of the Internet, along with its relationship with the Society, with particular emphasis on South-South dialogues and exchange. CIS has conducted extensive research into areas such as privacy, data protection, data security, and was also a member of the Committee of Experts constituted under Justice A. P. Shah.

CIS has submitted and published comments to the Draft Digital Information Security in Healthcare Act[1], The National Health Stack[2] as well as the National Digital Health Blueprint [3].CIS has also been cited multiple times in the Report of the Committee of Experts led by Justice Srikrishna.CIS values the fundamental principles of justice, equality, freedom and economic development. This submission is consistent with CIS' commitment to these values, the safeguarding of general public interest and the protection of individuals' right to privacy and data protection. Accordingly, the comments in this submission aim to further these principles. We welcome the opportunity provided to our comments on the Policy and we hope that the final Policy will consider the interests of all the stakeholders to ensure that it protects the privacy of the individual while encouraging a digital health ecosystem.

High Level Comments

- **The Personal Data Protection Bill(PDP) should be enacted prior to the introduction of this Policy**
  The Personal Data Protection Bill is being devised to act as the data protection framework of the country and thus any proposal or regulation to process health data which comes within the ambit of sensitive personal data should be subject to

[1]Mohandas, S.,&; Sinha, A. (2018, April 22). Comments on the Draft Digital Information Security in Healthcare Act. Retrieved September 21, 2020, from https://cis-india.org/internet-governance/blog/comments-on-the-draft-digital-information-security-in-healthcare-act

[2]Sarkar, T., Dasgupta, S., &; Barooah, S. P. (2018, July 31). Comments on 'National Health Stack : Strategy and Approach'. Retrieved September 21, 2020, from https://cis-india.org/internet-governance/files/CIS-NHS-Comments

[3]Prabhu, S., Tandon, A., Rathi, A., &; Sarkar, T. (2019, August 7). Comments on the National Digital Health Blueprint. Retrieved September 21, 2020, from https://cis-india.org/internet-governance/blog/samyukta-prabhu-ambika-tandon-torsha-sarkar-and-aayush-rathi-august-4-2019-comments-on-national-digital-health-blueprint

the prior enactment of the PDP Bill and the establishment of an independent Data Protection Authority. Several clauses of the PDP Bill, such as the definition of sensitive personal data, consent manager are included in this Policy without any explanation for the relationship between this Policy and the PDP Bill.

- **Clarity on the role of the State Governments**
  Under the federal structure of the Constitution, health is a state subject and therefore state governments would also have the right to regulate this policy. It is important that the state governments and state health authorities are consulted and their approval taken prior to the enactment of this Policy. Ideally, the views of the state government should also be circulated as part of this Policy.

- **Clarity on how this policy is situated between the NHS, the National Health Policy and the National Health Authority**
  The National Health Stack (**NHS)** released in July 2018 was stated to be "a visionary digital framework usable by centre and state across public and private sectors."[4] The NHS laid out provisions for the creation of National Health Registries, and the use of health data for furthering Ayushman Bharat. However this document does not state how this policy would fit with the National Health Stack, or clarify the status of the Health Stack. Further, as per clause 2(c), this policy will also be applicable to the National Health Authority (NHA) and the NHA shall be responsible for implementing this policy. The NHA is the authority responsible for implementing the Ayushman Bharat Pradhan Mantri Jan Arogya Yojana, and therefore it is unclear as to the basis on which the NHA will also be responsible for leading this policy.

- **Need for a clear definition and scope of Health data**
  The PDP Bill defines health data as "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 associating the data principal to the provision of specific health services"; however with the onset of the Covid-19 pandemic and the measures taken thereafter a number of organisations are now collecting health data. Hence this policy could have provided a detailed explanation of health data in the current context in order to ensure that organisations collecting any health data would be governed by the principles laid out in this Policy and the PDP Bill.

- **The role of the Data Protection Authority**
  The Policy is silent about the role of the Data Protection Authority (to be established under the PDP Bill), it does not specify whether the data principal will have the right to file complaints before it. It merely states that the data principal

[4] Niti Aayog. (2018, July). National Health Stack. Retrieved September 21, 2020, from https://niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf

should first approach the grievance redressal officer of the data fiduciary, and if the grievance is not redressed, then she should approach the Data Protection Officer and finally the Ministry of Health and Family welfare or the appropriate court. It is important to note that under the PDP Bill, the data principal has the right to directly approach the Data Protection Authority.[5]

- **Role of the Data Fiduciaries**
  Clause 17.1 of this Policy merely states that a data fiduciary wishing to issue a health ID can register with the NHA and obtain an authorisation key to access the services required for generation of a Health ID. No guidelines or any other information has been provided or referred to regarding the categories of data fiduciaries who will be eligible to register with the NHA to issue the health ID, and the eligibility requirement that such data fiduciaries need to comply with to be eligible to register with the NHA.

Clause Wise Comments and Recommendations

CHAPTER 4 Definitions

(a) **Anonymisation**: The policy defines anonymisation as "such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified through any means reasonably likely to be used to identify such data principal;"

Comments: The definition of the term "anonymisation" is the same as in the PDP Bill, and as mentioned by CIS in our submission we reiterate that the definition of anonymisation be changed in such a way that it balances the need to protect privacy while enabling scientific research and innovation.

Recommendations: We reiterate the recommendation made in our submission to the PDP Bill. "The term "irreversible" from the definition of anonymisation can be removed, in order to make provisions for the advancement in technology and research. This would also account for the challenges that exist with anonymization and the ability to re-identify individuals, as has been called out by many experts including the Sri Krishna Committee. In the current form, there are various exemptions tied to anonymised data, therefore, a high threshold is appropriate and may be applicable at a later stage if anonymisation procedures do in fact assure irreversibility in the future. Alternately, we can choose to borrow from the definition of anonymisation from the Brazilian Data

[5] Clause 53 (1) of the PDP Bill states that:" The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that—(a) the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interest of data principals; or any data fiduciary or data processor has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority."

Protection Bill which defines anonymised data as “data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing.” Another approach could be to require anonymisation through aggregation and once aggregated, personal data would no longer be protected under the PDP Bill. Aggregated data falls within the ambit of anonymised data, but could still raise concerns around community privacy and thus fair and reasonable processing obligations would still need to apply”.[6]

(c) **Child:** The policy defines “child” as “a natural person/individual who has not completed eighteen years of age”.

Comments:. The definition of the term “child” should evolve from the definition provided in the Indian Contract Act 1872, and the age where a child can give consent to data processing of their health data must not be equated with the conditions required for maturity as defined under the Indian Contract Act. This definition does not account for the realities of how health data of children are collected by multiple data processors.

Children interact with data fiduciaries from a much younger age than 18 and requesting age verification and parental consent can undermine a child’s ability to understand and choose how their data is being used. The GDPR under Article 8 states that in the processing of the personal data of a child shall be lawful where the child is at least 16 years old, where the consent is given or authorised by the holder of parental responsibility over the child. The GDPR also allows member states to lower the age to 13 years.[7]

Recommendations: We reiterate the recommendation made in our comments on the PDP Bill.The provisions of parental consent allow the data fiduciary to implement services that will be used by children without ensuring that the data of children are processed with care. Such a responsibility should be reflected in the definition and under the ‘privacy by design’ principle. This would also provide children and parents with stronger grounds for redress - which are currently limited to the existence of consent. With this obligation in place, the age of mandatory consent could be reduced and the data fiduciary could have an added responsibility to informing the children in the simplest manner how their data will be used. Such an approach places a responsibility on data fiduciaires when implementing services that use the health data of individuals under the age of 18 and allow the child to be aware of their rights as data principals.

(f) **Consent manage**r:Consent manager means an entity or an individual, as the case may be that interacts with the data principal and obtains consent from him/her for any

---

[6] Sinha, A., Hickok, E., Bedi, P., Mohandas, S., &; Rajwade, T. (2020, February 12). Comments to the Personal Data Protection Bill 2019. Retrieved September 21, 2020, from https://cis-india.org/internet-governance/blog/comments-to-the-personal-data-protection-bill-2019

[7] Sinha, A., Hickok, E., Mohandas, S., &; Basu, A. (2018, July 28). Comments to The Personal Data Protection Bill. Retrieved September 21, 2020, from https://cis-india.org/internet-governance/comments-the-personal-data-protection-bill

intended access to personal or sensitive personal data, where the role of the consent manager may be provided by the NHA or any other service provider.

Comments: The Policy states that the consent manager will interact with the data principal and obtain consent for any access to personal or sensitive personal data. The consent manager has also been defined as an entity or an individual. However, Clause 11.2 indicates that the consent manager can collect personal and sensitive personal data in case of obtaining electronic consent from the data principal.

Recommendations: The term consent manager that has been used in the Policy has also been referenced in the proposed data protection framework. The definition should be modified to classify them as data fiduciaries or processors to ensure the direct application of the data protection regulations once notified. The proposed framework requires the data protection authority to issue regulations on the manner and the technical, operational and financial conditions for registration of a consent manager. The policy states that the consent role of the consent manager will be determined by the NHA. It is recommended that cooperation between the NHA and the DPA in such matters be mandated as a requirement of the policy.

Sensitive Personal data: The Policy states that "for the purpose of this Policy, sensitive personal data would include information relating to various health conditions and treatments of the data principal, such as EMR, EHR and PHR;"

Comments: The addition of this sentence below the exhaustive list of sensitive personal data can be confusing especially when the definition of sensitive personal data includes "physical, physiological and mental health data" and "medical records and history". There should ideally be a clarification as to why there is a need to specify "information relating to various health conditions and treatments of the data principal, such as EMR, EHR and PHR;" in addition to the inclusion of medical records and history as sensitive personal data.

Recommendations: We recommend that either the sentence be removed or an explanation is included specifying the instances where EHR, EMR and PHR would be different from medical records and history and physical and mental health data.

Chapter II. Applicable Law and Governance Structure

Clause 6. Governance Structure

Comments: Clause 6 of the Policy states that the governance structure shall be specified by the National Health Authority (**NHA**) and shall consist of such committees, authorities and officers at the national, state and health facility levels as will be necessary to implement the NDHM. However, the Policy does not provide any details or guidance on how the NHA will constitute such committees and who will be the members of these committees, and also what will be the specific powers and responsibilities of these committees.

Recommendations: The Policy should clearly articulate the principles to be followed by the NHA while constituting the committees. It should either specify the role and responsibilities of each committee or at a bare minimum lay down the broad framework of each committee. The composition of each committee should also be specified, i.e. the number of members, the designation and the term of each member. The committees should consist of adequate members from civil society organisations, the representatives from the medical community (at the state and district level) and the necessary representatives from ministry of health and family.

Clause 6: The Policy also states that the Committee shall also consist of a data protection officer who shall be a government officer and who shall, in addition to the functions identified under this policy, communicate with regulators and external stakeholders on matters concerning data privacy and serve as an escalation point for decision making on data governance and other matters concerning data.

Comments: Vital oversight activities that will have a direct impact on the protection of privacy of the individuals have been delegated to the data protection officer. However, there isn't any guidance on the selection criteria for such an officer. The proposed data protection framework also refers to the position of the data protection officer and delegates the task of specifying regulations around the necessary qualification and experience required for such a position on the data protection authority.

Recommendation: It is recommended that either fresh guidance on the selection criteria for a data protection officer be provided under the policy or the provisions from the proposed data protection framework be referenced in the policy.

Chapter III. Consent Framework

Clause 9: Consent in relation to collection and processing of personal or sensitive personal data

Clause 9(1): The Policy states that data fiduciaries can collect or process personal or sensitive personal data only with the consent of the data principal. It is the responsibility of the data fiduciary to ensure that the consent given by the data principal is valid.

Comments: The policy places the burden of proof on obtaining a valid consent on the data fiduciary and lays down the characteristics of a valid consent in accordance with the proposed data protection framework.

Recommendations: The responsibility of ensuring valid consent is on the data fiduciary. However, there is no indication that such a responsibility will be operationalized. Language from GDPR on demonstrable consent can be borrowed to ensure that the data fiduciary is obligated to store the copies of consent for further scrutiny in the event of an investigation.

Clause 10: Privacy notice for the collection of personal and sensitive personal data

Comments: Clause 10.3 of the Policy stipulates the information to be included in the notice to be given to the data principal by the data fiduciary at the time of collection or processing of personal data. The contents of the privacy policy are similar to those stipulated in the PDP Bill, however, while PDP Bill states that the privacy policy should clearly inform the data principal about their right to file a complaint before the Data Protection Authority[8], the privacy policy articulated under this Policy is silent about it.

Recommendations: The information to be provided to the data principal in the privacy policy should clearly specify that the data principal has the right to file complaints before the Data Protection Authority as per the procedure prescribed in the PDP Bill.[9]

Clause 12: Processing personal or sensitive personal data pertaining to a child

Comments: The clause is silent on the status of the child's health records and the consent provided by their parents/guardians, once they have attained the age of majority.

Recommendations: The clause should include a provision which clarifies the rights the child will have towards their own data once they attain majority. This would be similar to the provisions in the Health Insurance Portability and Accountability Act (HIPAA) of the United States that allow the minor who has now attained the age of majority to exercise all the rights granted by the HIPAA Privacy Rule, including information which was consented for or provided by their parents/guardians on their behalf.[10]

Clause 12.3: This clause states that a valid proof of relationship and proof of identity of the parent is required to be submitted to the data fiduciary in order to verify the consent of the parent or guardian for processing the personal or sensitive personal data of the child as set out in paragraph 12.2 above.

Comments: The clause fails to understand the ever expanding organisations that are collecting health data, and the requirement of a valid proof of identity of the parent is a requirement that is both arbitrary and difficult to implement.

Recommendations: The clause could instead require the parent or guardian to attest or verify that they are indeed who they represent themselves to be and legal recourse should be undertaken for misrepresentation.

---

[8] Clause 7(1)(l) of the Draft Personal Data Protection Bill 2019
[9] Clause 53(1) of the Draft Personal Data Protection Bill 2019
[10] U.S. Department of Health & Human Services. (n.d.). When an individual reaches the age of majority or becomes emancipated, who controls the protected health information concerning health care services rendered while the individual was an unemancipated minor? Retrieved September 21, 2020, from https://www.hhs.gov/hipaa/for-professionals/faq/230/is-parent-rep-once-child-reaches-age-maturity/index.html

Clause 13: Processing personal or sensitive personal data of data principals who are seriously ill or mentally incapacitated

Comments: The clause is silent on the status of the rights of the data principal if they are no longer mentally incapitated or seriously ill.

Recommendations: Similar to the recommendation made in the clause above. The clause should include a clause which clarifies the rights of the person when they are no longer mentally incapaciatted or seriously ill. This would also be similar to the provisions in Health Insurance Portability and Accountability Act (HIPAA) of the United States that allows a person who has been emancipated to re-exercise all the rights granted by the HIPAA Privacy Rule, including information which was consented for or provided during their period on incapacity.[11]

Clause 14: Rights of data principals

Clause: 14.1(a)(iii): The data principal shall also have the right to access in one place the identities of all the data fiduciaries with whom her/his personal data has been shared by any data fiduciary together with the categories of personal data that has been shared.

Comments: The policy (Cl. 27.2) permits the data fiduciaries to engage data processors to process personal data on their behalf after conducting appropriating due diligence. Since the ecosystem will include data processors, the data principal should have the right to access the identities of those data processors with whom their personal data has been shared.

Recommendations: It is recommended that the identities of the data processors be provided to the data principal in line with Section.7 of draft Personal Data Protection 2019.

Chapter IV. ID Policy

Clause 16: Principle of non-exclusion for Health ID

16(4): It is clarified that no individual shall be denied access to any health facility or service or any other right in any way merely by reason of not being in possession of a Health ID or for not opting to participate in the NDHE.

---

[11]U.S. Department of Health & Human Services. (n.d.). When an individual reaches the age of majority or becomes emancipated, who controls the protected health information concerning health care services rendered while the individual was an unemancipated minor? Retrieved September 21, 2020, from https://www.hhs.gov/hipaa/for-professionals/faq/230/is-parent-rep-once-child-reaches-age-maturity/index.html

Comments: Including a non – exclusion provision is commendable. However, past experience with Aadhaar and a similar non -exclusion provision has indicated how they are not fully effective when the policies are implemented.

Recommendations: It is recommended that strict guidelines regarding non-exclusion be shared with all implementing institutions and individuals. In case evidence emerges of exclusion from welfare schemes or denial of service, it should be made mandatory to carry out an independent investigation should be carried out and implementing institutions be held liable for violating the fundamental rights of citizens, especially in case of public institutions. In addition, evidence-based research around the reasons for failure of earlier non-exclusion provisions be conducted and additional safeguards based on the research be included at the policy level to penalize or prevent any violations.

Chapter V. Obligations of Data Fiduciaries in Relation to Processing of Personal Data

Clause 26: Privacy principles to be followed by data fiduciaries

Comments: Clause 26.3 of the Policy, Privacy by Design, adheres to the 'Preventive not Remedial' principle, by prescribing the data fiduciaries to store the data of data principals in a federated and not centralised manner. The other recommendations of the Policy also allude to other principles of Privacy by Design such as 'Privacy by Default', 'Privacy Embedded into Design', and 'Visibility and Transparency'. However, it does not take into account some of the key principles, such as the 'Full Functionality – Positive-Sum, not Zero-Sum' principle[12]. Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. Privacy by Design rejects viewing these non-privacy objectives as trade-offs and accommodates them, in an innovative positive-sum manner[13].

It asks the data fiduciaries to make available a 'privacy by design' policy on its website, and details out the various categories of information that such a policy should contain. But, it lacks the specific directives towards how privacy by design should be followed in each of these categories. For instance, the policy asks for the obligations of the data fiduciaries to be stated, without more detail on what could such obligations be under the 'privacy by design' policy.

Recommendations: The policy should be more explicit in directing the data fiduciaries to adopt the privacy by design approach. It should give further steps to evaluate the data fiduciary's privacy by design policy. It should adopt the principles of privacy by design in

[12]Cavoukian, A. (n.d.). Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Retrieved September 21, 2020, from https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[13] Cavoukian, A. (n.d.). Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Retrieved September 21, 2020, from https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

clearer detail, including aspects such as accommodating all legitimate interests and objectives in a positive-sum manner, without making unnecessary trade-offs, applying data minimization and disclosure limitation, using accepted standards and frameworks, which are amenable to external reviews and audits, and wherever possible, carrying out detailed privacy impact and risk assessments.

Chapter VII: Grievance Redressal and Compliance

Clause 34: Compliance and Policy Governance

Clause 34.3: This Policy states that it shall be revised at least once every year. A copy of this policy together with any significant revisions shall be made publicly available on the NDHM website.

Comments: The periodic revision of this Policy is welcome, however the practicality of revising a policy in the same way as this Policy is being introduced (with a period of public consultation) would be difficult to achieve. Additionally the requirement for the stakeholders to which this policy is directed as to be not informed of the change in the policy could mean confusion and non-compliance to the revised policy.

Recommendations: The policy could be revised from time-to-time based on the changes in applicable laws and when the situation necessitates the revision or the addition of provisions. Additionally the policy should state that the revised guidelines would be intimated to the stakeholders, as well be publicly available on the website.