COMMENTS TO THE MINISTRY OF HEALTH AND FAMILY WELFARE ON THE **NATIONAL DIGITAL HEALTH MISSION: HEALTH DATA MANAGEMENT POLICY, 2020**

Siddharth Manohar
Senior Research Associate, Aapti Institute

The National Health Data Management Policy, released under the National Digital Health Mission, seeks to build a regulatory structure around the sharing, processing, and governance of health data in India. In this piece, we explore a few of the issues that the policy runs into in creating this framework, namely how it understands consent and access to data, as well as its approach to user privacy and governance over access permissions.

Consent and Data Principal Rights:

A lot of the rights afforded to end users are aligned to rights available under the Personal Data Protection Bill: rights of access to their information available with a fiduciary, and details on what entities this information has been shared with; a right to correct or erase that information; and a limited right to data portability, subject to an unspecified test of "technical feasibility" seemingly determined by the fiduciary.

The operation of consent requirements also follows the PDP Bill, allowing for 'consent managers' to act as intermediaries and process health data collected under the policy. The concept of consent managers can also be traced back to the PDP Bill, which defines it as "a data fiduciary which enables a data principal to gain, withdraw, review and manage their consent through an accessible, transparent and interoperable platform".

Now, the purpose of the consent manager as per the PDP Bill is to aggregate and manage consent information for users – this may include the list of fiduciaries with which data is shared, the specifics of data shared with each party, and the duration of these permissions. The consent manager as defined by the Bill however is not intended as an intermediary for the actual data that is being shared – the policy mistakenly uses this concept to frame consent managers as intermediaries that handle the health data themselves. The PDP Bill however makes it clear with the definition

of consent managers that this is not intended to be the case. The policy therefore needs to account for this and alter the language used in paragraph 11.2 accordingly.

Consent managers handling health data presents a unique problem of the creation of powerful intermediaries which not only control access to data but enjoy that access themselves – in a market where third parties approach them for access to health data, they become gatekeepers for access to this data, a role not intended for them under the policy.

Governance of access permissions:

The policy has taken the approach of creating a governance structure based on responsibilities assigned to authorities. As an approach to designing a governance system, this can work if there are clear channels of access and communication for users to redress grievances with respect to their health data and its usage under the NDHM. Accountability and implementation of accessibility measures has historically however been lacking in centralized projects, and this may be countered by providing clear and accessible channels of accountability, or else by providing users with the tools to manage their data themselves. The policy relies on the NHA to carry out a supervisory role over the entire regulatory structure proposed by the policy – it is not clear that the resources to over see the continued operations of a national system of data sharing are currently present in order to create an effective framework for empowering users and other stakeholders to share health data.

For example, the policy takes the following approach to governance of access permissions over anonymised health data:

> *"The NHA shall set out a procedure through which any entity seeking access to anonymised or de-identified data under this Policy will be required to provide relevant information such as its name, purpose of use and nodal person of contact and, subject to approval being granted under this procedure, the anonymised or de-identified data under this Policy shall be made available to such entity on such terms as may be stipulated in this behalf."*

Significantly, the NHA is tasked with responsibilities on data sharing – it is given powers to decide who gets to access health information from users whether anonymised or not – it sets out the procedure for this process, which leaves a crucial element of governance excluded from the policy. The contents of this procedure will be crucial to determine the governance of health data. Access and permission protocols, and verification of parties with whom data is shared, play a fundamentally important role in the process of data sharing. The policy must engage on the procedure for authorization to access health data processed by fiduciaries, particularly at the stage of broader drafting of the process.

The policy presumes that data may be successfully anonymised – ie, that a dataset may be converted such that no individual may be "reasonably likely" to be indentified from it. Anonymisation as a watertight possibility continues to bring up debate, with claims on the increasing efficacy of techniques to deanonymise data, to the extent that a question now exists as to whether there really may be said to be a data type identifiable as materially 'anonymised'. These de-identification and anonymisation techniques normally follow industry standards and may be adapted as required. Even with these protections however, protocols on permissions sharing controls need greater clarity for it to be effective in preserving user privacy.

Consent for processing of anonymised data:

The policy mentions the purposes of sharing of anonymised data as those of "facilitating health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions", and "such other purposes as may be specified by the NHA". The policy does not go into further explanation or quantification of these other purposes. There is nonetheless an ever-growing need for data in medical research – and the policy seeks to feed that demand by enabling sharing of medical data by fiduciaries through the structure NHA oversight and the framework of consent managers. Consent managers here however only apply to personal information – not to anonymised data. The policy does not contemplate the possibility of obtaining consent for sharing of anonymised data. This is significant because of the recent Report by the Committee of Experts on Non Personal Data which explicitly addresses this question:

> *"The Committee recommends that the data principal should also provide consent for anonymisation and usage of this anonymized data while providing consent for collection and usage of his/her personal data. Also, the Committee recommends that appropriate standards of anonymisation be defined to prevent / minimize the risks of re-identification."*

The NPD Report recommends that the sharing and use of anonymised non-personal data also be based on user consent, a principle which is not reflected in the Health Data Management Policy.

In closing, the draft needs to account for these issues, amongst others, with concerns of accountability, consent, user interests, and the collective privacy of all Indian citizens hanging in the balance.