National Health Authority

Ministry of Health & Family Welfare

Press Release (14.09.2020)

(In response to the report titled "Draft NDHM Policy: Experts warn of 'structural problems', lack of clarity on patient control over data" published on 14.09.2020 in The Indian Express which can be accessed at https://indianexpress.com/article/business/draft-ndhm-policy-experts-warn-of-structural-problems-lack-of-clarity-on-patient-control-over-data-6594847/lite/)

Before publishing the story, the views of the National Health Authority were not sought. Therefore, the National Health Authority is issuing the following clarification.

It may be noted that the Policy is at the draft stage and all comments/ feedback shall be considered before finalizing the draft Policy.

The following is a point-by-point response and facts being shared against certain perspectives and arguments mentioned in the Indian Express report *(in italics)*. The expert opinions mentioned in the report have misconstrued the draft Policy.

1. *One of them by Raman Jit Singh Chima, Asia policy director and senior international counsel at Access Now, states that, "the current draft policy has "structural" problems… (it) is a policy document issued under no statutory framework and on a topic that partly impacts India's federal structure, because health is a state subject. Not only can it not bind the state, it also isn't binding on the National Health Authority (NHA) that is enforcing it — the policy can be changed," said Chima.*

NHA Response – This is not correct. There are various laws and Supreme Court judgements that provide a comprehensive legal framework data security and privacy. The National Digital Health Mission follows a "privacy by design" approach to ensure that standards followed to protect patient information and the privacy of their personal health data are of the highest order. The draft Health Data Management Policy ("**draft Policy**") has been drafted keeping in mind the core tenets of privacy, security, and consent. The draft Policy has been developed under the statutory framework of existing laws such as the IT Act, Aadhaar Act, and judgements by the Supreme Court on data privacy and data security. Further, the draft Policy also draws from the Personal Data Protection Bill.

The participation in NDHM by all players, including States and UTs is voluntary. Thus, it is a consent-based arrangement. It is incorrect to state that the Policy would not be binding on the National Health Authority (Para 2.c).

The NDHM has its foundation in the National Health Policy, 2017 ("**National Health Policy**") and intends to work towards digitisation of the healthcare ecosystem of India. This would be done by creating digital health records and creating and maintaining registries for healthcare professionals and health facilities in order to ensure a smooth interoperable framework for the multiple partners associated with healthcare delivery to individuals in India. The National Digital Health Blueprint, 2019 (**NDHB**") recommends that a **federated architecture** be adopted, instead of a centralised architecture for the management of health data to ensure

interoperability, technological flexibility and independence across the National Digital Health Ecosystem ("**NDHE**").

To that end, this draft Policy is the first step in realising NDHM's guiding principle of "Security and Privacy by Design" for the protection of individuals' data privacy. It acts as a guidance document across the NDHE and sets out the minimum standards for data privacy protection that should be followed across the board in order to ensure compliance with relevant and applicable laws, rules and regulations.

2. *The policy puts the onus on the individual to understand whether they should consent to giving their data, but there is no clarity on whether it will be in a format that is easy to understand, according to CIS programme officer Shweta Reddy, who has also been studying the draft.*
   "Under this policy, it is unclear whether you will be notified each time your data is being used, and it is unclear who will enforce that," he said (Raman Jit Singh Chima).

NHA Response – Consent will be informed and detailed. Since the data will be accessed only after the consent, separate notification during the use is not required. In addition, there will be provision for sharing only part of data and that too only for a limited period of time. Further, the consent can be revoked even before the expiry of such time. The draft HDM Policy clearly defines the nature of consent and the applicable laws (Para 9.2), and also the requirement for fresh consent for any new or previously unidentified purpose (Para 10.2).

3. *"If I'm a law enforcement agency wanting to access your entire pharma records, who sold you what and for what purpose, I could go ahead and do that. There is no remedy mechanism and enforcement structure to prevent that from happening," he added.*

NHA Response – The legal authority of various authorities including law enforcement agencies shall remain the same, even after the approval of this draft Policy. The scope of legal authority cannot be changed by way of a Policy.

4. *Problems also arise where the ability of an individual to ensure their data is erased is concerned. "With respect to erasure, the policy provides only certain circumstances where the personal data can be erased," said Shweta Mohandas, policy officer at Centre for Internet and Society (CIS), who has been studying the draft closely. This is true even if the patient withdraws their consent, according to Murali Neelakantan, lawyer and former global general counsel for Cipla and Glenmark Pharmaceuticals.*
   "The policy allows the patient to only request that their data be erased if they're withdrawing their consent, but this request can also be denied. This doesn't give the patient the right or control over their own data, because there is no right to be forgotten in this policy," he told The Indian Express.

NHA Response – As per the current legal framework, even now the individual cannot demand destruction or erasure of data stored in the custody of health providers like hospitals. This provision exists because hospitals and other health providers need to store such data for a certain period of time for legal purposes. However, at the same time, the individual has the Right to Privacy, subject to various laws as far as this data in the custody of health providers is concerned. This legal framework protecting privacy shall continue to remain in force.

In addition, as far as data stored with the individual in personal health records is concerned, he/she shall be able to erase the whole data.

In addition, certain additional provisions are proposed in the draft pertaining to data stored by data fiduciaries eg. health information providers. This is an additional element of data privacy proposed to be provided as per the draft, over and above the existing legal provisions.

As defined in **Para 14 – Rights of data principals**: individuals may delete their own data, and also request data fiduciaries to delete any records stored with them, provided permitted by law. In instances where erasure might not be possible, provisions for over-writing, anonymisation or other method(s) of removal of the personal data from live systems have also been made in the draft Policy. Furthermore, in the event of the rejection of any erasure request by the data fiduciary, a written response will need to be provided (Para 14.2.d). This response can also be disputed by the individual and appropriate legal framework on their rights will apply. This is an improvement over the existing situation which does not provide any remedy for refusal for erasing certain data.

5. *"(It) also doesn't specify which database will contain the patient's information," Neelakantan added.*

NHA Response – As defined in **Para 26.3 – Privacy by Design**: "… The federated design of the NDHE ensures personal data of the data principals will be held at the point of care or at the closest possible location where it was created, with no centralised repository …". Hence, the medical data of individuals will not be stored by the NHA or any other central database, and will exist as part of the federated design, while being compliant with NDHM's security and privacy requirements.

6. *The definition of a consent manager is also not clear enough in the current policy to understand whether the role will be played by a private firm, NGO or government body, according to her. Certain clauses of the policy suggest that the consent manager will also be able to collect and process personal and sensitive personal data for particular purposes that are not specified. "We don't know if, apart from just taking consent, whether they will have access to personal and sensitive personal data. If a consent manager is supposed to help an individual exercise their rights against a data fiduciary, who is going to help them exercise their right against the consent manager," asked Reddy.*

NHA Response – The NDHM seeks to create a digital ecosystem in which the entire flow of data from origin to destination will take place electronically. Since, as prescribed in the draft Policy, the flow of data is consent-based, the consent manager as illustrated in the draft Policy has to be implemented at the level of the digital system. NDHM uses the electronic consent framework from MeitY to manage consents. This consent manager is 'an electronic system' which manages the consent. To begin with, such a software service for the consent manager will be provided by the National Health Authority. The decision regarding the participation of private entities for the purposes of said services will be taken at the appropriate stage. RBI has created similar electronic consent managers in the financial space (called Account Aggregators). Digital consent managers will only act as intermediaries for obtaining and transmitting consent between individuals and healthcare providers, they will not have access to any individual's health records in this process.

***