September 21, 2020

To
Shri Rajesh Bhushan
Secretary (Health and Family Welfare),
Union Ministry of Health and Family Welfare,
Government of India,
New Delhi.

CC:
Shri Indu Bhushan
Chief Executive Officer,
National Health Authority,
Government of India.

Subject: Access Now's submission to the call for comments on the Draft Health Data Management Policy of the National Digital Health Mission for India

We write to you in connection with the call for comments from the Ministry of Health and Family Welfare (MoHFW) and National Health Authority (NHA) regarding the Draft Health Data Management Policy of the National Digital Health Mission for India. We write to you to provide our comments based on our expertise working on different digital identity programmes and data protection laws across the world.

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 13 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT. We also have special consultative status at the United Nations.[1]

We also facilitate the #WhyID community - a community of more than 200 organisations and experts from across the world working towards ensuring that digital identity programmes respect

[1] Access Now, *About us*, https://www.accessnow.org/about-us/.

the rights of users.[2] This community has also led an open letter to international organisations and governments, expressing their concerns and asking some primary questions which help in ensuring that digital identity programmes are designed and implemented to ensure the protection of user rights. Recently, we released a discussion paper on digital health certificates in the context of COVID - 19 to look at the human rights impact of such certificates.[3]

At the outset, we would like to thank the MoHFW for inviting comments, holding these consultations, and we appreciate the opportunity to provide inputs and we hope that these will be helpful to the MoHFW in thinking through the National Digital Health Mission. We appreciate the extension of the original week deadline for comments by the MoHFW after repeated calls from civil society; however we respectfully submit that this consultation period has been far too short for this important topic and fell short of the best practices that should have been followed - both in terms of international approaches towards policy making on health data as well as the Government of India's own initiatives towards transparent, effective policy making - including the Pre Legislative Consultation Policy. Open, transparent and comprehensive consultations are an essential backbone of any public policy discourse. We hope that the MoHFW and NHA consider this in their further policymaking actions on this topic, including further public consultation and expert, stakeholder engagement before further advancing any health data management related policy or regulatory measures.

Below we provide our substantive comments on the Draft Health Data Management Policy.

1. **The present consultation scope is limited and needs to be broadened**

It is very important that for comprehensive review, the whole ecosystem be made available for review. Important policies such as Information Security policy, and Data Retention and Archival Policy, along with many other proposed policies that would impact the health ID and health data collection and management are mentioned in these documents but not been made available for review and comment at present. Their interaction with the health data management policy is extremely important to understand the working and impact of NDHM.

2. **Health data management should not be governed solely by a 'policy' document that places both scheme deployment and regulation burdens on the National Health Authority**

The current draft document provides a policy for the Government of India. This policy, among other things, deals with the rights and obligations of the multiple functionaries envisaged under the National Digital Health Mission. While a policy document is beneficial in providing the general direction and vision of the Union Government on several fronts, rights of users must be

[2] Access Now, #WhyID, https://www.accessnow.org/whyid/
[3] Access Now, #WhyID: Digital health certificates are not immune from violating users' rights, https://www.accessnow.org/whyid-digital-health-certificates-are-not-immune-from-violating-users-rights/

provided in robust law with adequate avenues for redressal. It remains unclear whether there shall be a followup regulation or law proposed by the Union Government.

The current framework envisaged under the NDHM does not sufficiently protect the rights of individuals; that includes their rights relating to privacy and data protection around their health data, but also wider human rights and constitutional remedy. The National Health Authority has been constituted under an executive order and its own legal status in running this proposed scheme and managing the collection, use, and regulation of health data of residents from states across the breadth of the country is potentially circumspect with regards to the provisions of the Constitution of India. The NHA is envisaged as being the implementing, regulatory as well as adjudicatory body under the NDHM. Under the current framework, the NHA would have too many roles and a clear conflict of interest in managing the NDHM. The Government of India is the largest collector of health information in India, which makes the need for an independent regulator all the more important for any health information ecosystem.

It would be hugely helpful if such clarification is provided by the Union Government, and the robust legislation is passed by the Parliament of India to support the rights of users. This is even more important given that health is a subject primarily given to the states under India's federal constitutional structure, and clarity on how state government usage of health identity and data relates to any Union Government measure will likely require a law passed under the relevant constitutional framework, and not just a mere executive policy.

3. Indian Government measures towards managing and regulating health data must follow the enactment and enforcement of a comprehensive data protection and privacy law

India, the largest democracy in the world and second-largest internet user base, has been trying to enact a national data protection law for quite some time now. The Personal Data Protection Bill, 2019 (PDP Bill) which has been approved by the Union Cabinet and was placed in the Lok Sabha (lower house of the Indian Parliament) is currently under review to a Joint Parliamentary Committee - consisting of members from the Lok Sabha (Lower House) and Rajya Sabha (Upper House).

The vision of the National Digital Health Mission, at its centre, is a vision of creating a platform for the health data of 1.3 people of India. Health data is deeply sensitive and personal to a person. It is important that a platform of this scale be adequately protected and regulated by an independent data protection and privacy authority. No such authority or law exists in India at the moment. The current draft of the PDP Bill envisages sectoral regulations, which are formed in consultation with the Data Protection Authority (DPA) formed under the PDP Bill. Creating sectoral policies which are not made in consultation with an independent DPA and may be in conflict with the policies and regulations of the DPA is not advisable. It may lead to the creation of multiple sources of truth for government departments and private sector actors. It is essential

that regulations and policies are streamlined in India, wherein general principles and regulations are derived from a robust, independent data protection authority and sectoral regulations are made in consonance with the guidance of such regulations and under advice of the DPA.

The language of the present policy creates confusion with the substantive rights and mechanisms proposed to be created by the PDP Bill and may result in implementing government agencies, medical stakeholders, private sector participants, and everyday patients and citizens being likely confused and in conflict. A policy document with no clear statutory basis or authority from subordinate law making powers does have the effect of law, which means that it would not be able to create substantive legal duties upon non governmental entities.

The Digital Information Security in Healthcare Act (DISHA) was proposed in 2018 by the government of India for this very purpose - to secure the healthcare data of patients in India. It also envisaged rights and remedies for patients. However, it seems that this effort was postponed to ensure that such a sectoral law is only passed after a general law for data protection and privacy is passed in India. The Government of India should clarify the interaction between the DISHA Act, this policy document and the PDP Bill. This policy document may not be effective in a vacuum and proper backing of the PDP Bill and a sectoral law would be required to ensure that the policy document has efficacy. However, if this policy is being enacted for reasons of expediency and emergency, then a compelling, critical purpose must be stated by the Union Government. Further, such measures should be given a clear sunset period and folded into the data protection law.

4. **The current definitions used by the draft Health Data Management Policy conflict with the terms in the Personal Data Protection Bill and earlier draft DISHA Bill**

There are significant deviations in the definitional and substantive provision text in the current health data management policy from comparative provisions in the PDP Bill and the draft DISHA Bill. Several of these deviations appear to reduce the space for rights of users and raise other concerns; we highlights some of these in the following table:

Health Data Management Policy	PDP Bill and draft DISHA Bill	Impact
“anonymisation” in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified through any	**PDP Bill:** "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which	The standard used in the definition of anonymised data has been amended from the standard provided under the PDP Bill, 2019. Under the PDP Bill, the standards of

means reasonably likely to be used to identify such data principal;	meets the standards of irreversibility specified by the Authority	irreversibility seems to be based on the standards established by the proposed data protection authority, while the standards under this policy seem to be based on standards established by the government of India, along with a “reasonableness” standard under the definitions.
“personal data” means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information. For the purpose of this Policy, personal data would include Health ID and Personal Health Identifier;	**PDP Bill:** "personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; "sensitive personal data" means such personal data, which may, reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier;....	The Health Data Management Policy dilutes the definition of personal data by excluding inferences drawn from personal data from within the ambit of personal data. Given that the derived data is based on the personal data, it must be within the ambit of personal data, as it too contains information which can identify an individual along with being essential to the privacy of an individual. Further, under the Health Data Management Policy Health ID is treated as personal data and not sensitive personal data. The PDP Bill treats “official identifiers” as sensitive personal data and a Health ID would come within the ambit of official identifiers. This change in definition again dilutes the standards set under the PDP BIll 2019, and lessens the safeguards given to an individual in relation to their official identifiers issued by the state.

“health facility” refers to health facilities across the country such as hospitals, clinics, diagnostic centres, health and wellness centres, mobile vans, ambulances, pharmacies etc.;	**DISHA Bill:** Clinical Establishment’ means (i) a hospital, maternity home, nursing home, dispensary, clinic, sanatorium or an institution by whatever name called offers services, facilities requiring diagnosis, treatment or care for illness, injury, deformity, abnormality or pregnancy in any recognised system of medicines established and administered or maintained by any person or body of persons, whether incorporated or not; or (ii) a place established as an independent entity or part of an establishment referred to in sub-clause (i), in connection with the diagnosis where pathological, bacteriological, genetic, radiological, chemical, biological investigations or other diagnostic or investigative services with the aid of laboratory or other medical equipment, are usually carried on, established and administered or maintained by any person or body of persons, whether incorporated or not, and shall include a clinical establishment owner, controlled or managed by a. the Government or a department of the Government; b. a trust, whether public or private; c. a corporation (including a society) registered under a Central, Provincial or State Act, whether or not owned by the Government; d. a local	While the Health Data Management Policy defined health facilities, the DISHA Bill treats similar establishments as Clinical Establishments. This is an important distinction, as clinical establishments are regulated entities by law, whereas health facility is a vaguely defined term allowing non-regulated entities to qualify under the law and be able to get access to health information and become important stakeholders in the NDHM ecosystem.

	authority; e. a single doctor, but does that include the clinical establishments owned, controlled or managed by the Armed Forces. Explanation: For the purpose of this clause, “Armed Forces” means the forces constituted under the Army Act, 1950 (46 of 1950), the Air Force Act, 1950 (45 of 1950) and the Navy Act, 1957 (62 of 1957)	

5. The draft policy fails to account for known implementation issues that would impact resident freedoms and inclusion

It is highly encouraging to see that at various instances the policy clarifies that participation in the National Digital Health Ecosystem is purely voluntary and 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 National Digital Health Ecosystem.

Any policy, law or regulation is only as good as its implementation. Lack of state capacity, confusing architecture, lack of political will, and corruption become some of the impediments in translating words to on ground realities. As mentioned above, the lack of clarity of the legal efficacy of this policy and its interaction with the PDP Bill may create confusion in implementation for government agencies and private sector actors. Users would be hard-pressed to exert their rights and seek remedies in such a scenario. As we have seen time and again in the case of the Aadhaar programme, even while many use cases of Aadhaar remained voluntary, the actual implementation showed otherwise, where users were denied service and misinformed that use of Aadhaar is mandatory. In order to allay these concerns, an important step may be to provide clear alternate mechanisms for users not opting in to the National Digital Health Ecosystem within this policy.

Further, a national digital health ecosystem requires efficient and working underlying technology infrastructure to work across India. This would not only be essential for the smooth functioning of the ecosystem, provision of medical services to citizens of India, but also to ensure that the data and rights of users are protected. Without adequate technology infrastructure, the implementation of the national digital health ecosystem would not be possible, and may even lead to de-facto exclusion of those without adequate access to such infrastructure.

6. The problem with the sharing of anonymised data

The policy provides that anonymised data by data fiduciaries may be made available to many institutions for various purposes such as statistical analysis, research, and development of diagnostic solutions. While the intent of the provision seems to be to promote research activities, the result of the provision may be to open up users to exploitation. Existing research has found that in many instances anonymised data can be very easily used to re-identify individuals.[4] Further, the methods of de-identification or anonymisation are required to be as per protocols developed by the government of India. The pace of the movement of technology and its use for re-identification would be too high for hard coded regulations to be able to keep them in check over time.

It is encouraging to see that the policy provides that re-identification of individuals would be prohibited. In practice, however, it would become highly difficult to track and find instances of re-identification when the underlying anonymous data is being freely shared.

7. The role and purpose of Health Information Users must be clarified

Under the NDHM, Health Information Users (HIU) have been identified as entities which would get access to patient data from other entities (Health Information Providers), on the basis of consent obtained from the patient. Under the policy, there are no checks and balances placed on the HIU for getting access to the data of the patient, apart from getting consent from the user. HIUs act as secondary data fiduciaries with no direct contact with the data principal. The role and purpose of HIUs must be clarified and additional legal obligations must be put on HIUs regarding the use of the data along with ensuring that simple consent based on lengthy forms does not create an infrastructure where private health records are passed in an ecosystem without any care.

8. Lack of controls around surveillance and access to information by government agencies

Along with financial data, health data as envisaged under the National Digital Health Ecosystem, probably constitutes the most sensitive information. Surprisingly, there is no provision which provides checks and balances against governmental access to such data. The Srikrishna Committee report for the Personal Data Protection Bill and the *Justice K.S.Puttaswamy vs Union Of India* provide great appraisal and critique of the surveillance architecture present in India along with the need for surveillance reform. Under the National Digital Health Mission, the government acts as an active functionary and has access to a huge amount of health data of citizens of India. It is essential that adequate checks and balances, founded on the principles of necessity and proportionality and adjudicated by an independent

[4] Wired. Anonymized Phone Location Data Not So Anonymous, Researchers Find, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/

judicial authority, be specifically established to ensure that the national digital health ecosystem does not render itself to abuse to establish a permanent health surveillance infrastructure.

9. **Insufficient information on cybersecurity status of a health identity and data system**

The current policy fails to elucidate a sufficient data breach mechanism for this system; ideally this should match and build on the proposed data breach provision in the PDP law. Any health data breach must be required to be immediately disclosed to the Data Protection Authority in coordination with relevant authorities such as the NHA. Data breach notification must be mandatory - whether by private sector or government entities, including the NDA - and users must be required to be immediately notified. Additionally, the scheme should make clear whether any health identity system and government health data storage constitutes critical infrastructure, and the role of existing cybersecurity institutions such as CERT-IN and the NCIIPC.

10. **Proposed grievance redressal mechanisms are insufficient and will clash with the Data Protection Authority**

The grievance redressal officer envisaged under the policy - NDHM-DPO - seems to lack structure, independence and scale. The government of India plays a huge role as a fiduciary in the National Health Data Mission. In many instances, the grievance of users may be against the actions of the government and its handling of the user's data. The NDHM-DPO is an officer of the union government, and may not possess the independence and wherewithal to deal with complaints against the union government.

Given that the current draft is a policy by the government, the rights and obligations created under the policy may not be enforceable against private entities. It is important that an enforceable and comprehensive rights based framework be established, which is implemented by an independent and strong authority.

The current flow of complaints under the grievance redressal process is not clear. A complaint made to the data protection officer of the data fiduciary may be referred to arbitration on the basis of an inter-se agreement between the user and the data fiduciary, which may prove to be cumbersome and expensive for the individual. Legal remedies based on contract are always available under any contractual relationship, but it is essential that the rights based policy framework provide cost effective and fast remedies which are based on legal rights under law and regulations.

Conclusion

In conclusion, we would like to thank you for the opportunity to provide inputs into the consultation. It is important that laws, regulations and policies established to govern data are based on a rights based approach for users. Such frameworks must be clear, comprehensive

and enforceable. A general data protection framework with an independent data protection authority would provide a solid foundation for sectoral regulations. Leapfrogging to complex sectoral regulations without the existence of a horizontal data protection law and authority may only create complex, and confusing legal frameworks which render themselves to disuse during implementation.

We respectfully submit that given the many concerns and challenges that are currently there with the proposed project, the government should seek to answer the questions of stakeholders and conduct a further consultative process along with proposing the additional regulations or proposed measures under the Data Protection Act regarding health data when enacted. If any standalone temporary regulations or legal measures on health data are proposed, a sunset period and review process should be included at the outset.

We stand available and ready to answer any questions regarding our submissions here, along with providing any assistance as may be required.

Sincerely,

Naman M. Aggarwal
Global Digital Identity Lead and Asia Pacific Policy Counsel, Access Now
naman@accessnow.org

Raman Jit Singh Chima
Asia Pacific Policy Director and Senior International Counsel, Access Now
raman@accessnow.org