Comments to the Draft National Health Data Management Policy 2.0

21, May, 2022

This is a joint submission on behalf of (i) Access Now, (ii) Article 21, (iii) Centre for New Economic Studies, (iv) Center for Internet and Society, (v) Internet Freedom Foundation, (vi) Centre for Justice, Law and Society at Jindal Global Law School, (vii) Priyam Lizmary Cherian, Advocate, High Court of Delhi (ix) Swasti-Health Catalyst, (x) Population Fund of India. The list has been arranged alphabetically.

At the outset, we would like to thank the National Health Authority (NHA) for inviting public comments on the draft version of the National Health Data Management Policy 2.0 (NDHM Policy 2.0) (Policy) We have not provided comments to each section/clause, but have instead highlighted specific broad concerns which we believe are essential to be addressed prior to the launch of NDHM Policy 2.0

High-Level Comments and Recommendations: **2**

- Prerequisites of a digital health records system 2
- Absence of a Data Protection Law 2
- Concerns over vague language/terminology used in the Policy 3
- Lack of clarity on the proposed structure of the National Digital Health Ecosystem 4
- Absence of any legislative mandate to the Health Data Management Policy 4
- Definition of Sensitive Personal Data Needs to be in-line with the Data Protection Bill 5
- Need to make the Policy and its Implementation easily understandable to healthcare professionals 6
- Reliance on digital infrastructure needs to be examined 7
- Need for more detailed privacy and security by design policy 8
- Need for a More Adequate Governance Mechanism 9
- Need Clarity on Role of Health Information Exchange & Consent Manager 10
- Opportunity to Withdraw Consent for Child on Attaining Majority or Person no Longer Being Incapacitated 11

Need for a Robust Grievance Redressal Mechanism 12
Concerns Regarding the Unique Health ID 13
Confidentiality and Consent 14
Exclusion errors and 'coercion-based inclusion 14

High-Level Comments and Recommendations:

1. Prerequisites of a digital health records system

We recommend that a thorough understanding and evaluation of the health system and the capacity of the system to implement such a digital health system should be undertaken prior to the rollout of the second version of the Policy- this also includes examining the legal foundation/basis of such a Policy.

2. Absence of a Data Protection Law

The current draft version of the Health Data Management Policy has once again been published in the absence of a comprehensive data protection law. The revised version of the draft policy similar to the previous version appears to be a patchwork of the Data Protection Bill currently pending before Parliament. Several policies and guidelines relating to the health sector such as the Health Data Retention Policy[1], the Telemedicine Guidelines, 2020[2], the Health ID notification, 2021[3] (pursuant to the Health Data Management Policy) has been released and notified in the absence of any comprehensive specific legislation governing health data.

We recommend that the Policy should be finalised only after either a Data Protection Bill or separate legislation governing health data has been passed by Parliament. A policy does not have the same force of law as legislation which undergoes parliamentary scrutiny.

---

[1] Ayushman Bharat Digital Mission, *Draft Health Data Management Policy*, Version 2.0, April 2022, available at https://abdm.gov.in:8081/uploads/Draft_HDM_Policy_April2022_e38c82eee5.pdf Clause 2 of the Policy (Last visited on May 21, 2022).
[2] Telemedicine Practice Guidelines, Enabling egistered Medicial Practitioners to Provide Healthcare Using Telemedicine, March 25, 2020 available at https://www.mohfw.gov.in/pdf/Telemedicine.pdf (Last visited on May 21, 2022).
[3] Unique Health Identifier Rules, 2021.

3. Concerns over vague language/terminology used in the Policy

The Policy reflects the gender binaries in the language that has been used to identify data principal. Data Principals or any other individuals have been referred or identified by using the pronoun he/him or she/her. It does not reflect the identity of the transgender community- there is no identification or use of the pronoun 'they/them'.

The Transgender community has been recognised and legal status by virtue of the Supreme Court judgement in *National Legal Services Authority of India v Union of India* and by the enactment of the Transgender Persons (Protection of Rights) Act, 2019 and we recommend that the language in the Policy be suitably modified and amended.

Similarly with respect to persons with disabilities, while the Policy mentions accessibility for the healthcare workers, there is no mention of accessibility for persons with disabilities. This seems like a missed opportunity as the Policy should ideally clarify certain provisions in detail, especially for individuals who might benefit the most from accessible healthcare systems.

Additionally, the use of the term "mental incapacity" which is neither defined in the Policy nor the Mental Healthcare Act and the use of vague terms could have serious consequences for people who might lose the autonomy over their bodies and data based on this provision. We recommend that the definition be made in line with the Mental Healthcare Act.

We recommend replacing the term "mental incapacity" with the terms 'mental illness' or 'mental retardation' as defined by the Mental Healthcare Act, 2017. Inclusion of the following proviso and explanation after Clause 13(2):"Provided that in the event that neither the nominee nor the data principal is able to provide valid consent, only personal information that is required to save the life of the data principal shall be collected and processed.""Explanation: The medical opinion of a healthcare worker, which shall be formed in good faith, should be the only relevant consideration in ascertaining whether the data principal is facing a threat to life or a severe threat to health."

4. Lack of clarity on the proposed structure of the National Digital Health Ecosystem

The Policy has been proposed as a first step in establishing a National Digital Health Ecosystem (NDHE). As per the Policy, participation in the NDHE is not mandatory and is based on the consent of the concerned individuals, healthcare professionals and health facilities. They will also have the option of 'opting in' or 'opting out' of the NDHE. However, there is no clarity on the mechanism to 'opt out' of the NDHE, and the consequences of exercising such an option.

As per clause 2(b), the Policy applies to "h*ealthcare professionals, including but not limited to doctors or healthcare practitioners (including those practicing recognised Indian systems of medicine such as Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homoeopathy), nurses, laboratory technicians, and other healthcare workers"* The inclusion of "other workers" requires definitional explanation. Does this include ASHA and Anganwadi Workers, considering that they are the frontline workers in India's healthcare system and are the first point of contact between the community and the healthcare system? There are also other health workers who work through various non-profits and other service providing agencies such as the HIV and Tuberculosis programs. This is exacerbated by the absence of any legislative mandate to the Policy- which is explained in the following points

5. Absence of any legislative mandate to the Health Data Management Policy

Similar to the digitisation of the healthcare sector there is no legislative backing to the Health Data Management Policy. It has emerged from the National Health Policy, 2017. The NHP recommended the creation of the National Digital Health Authority (NDHA) to regulate, develop and deploy digital health across the continuum of care. In 2018, the first attempt to create and establish the NDHA was through the enactment of the Digital Information Security in Healthcare Bill (**DISHA Bill**). However, the Bill has not yet been introduced in Parliament. Simultaneously in 2019, Niti Aayog proposed the National Digital Health Blueprint. The Blueprint recommended the creation of the National Digital Health Mission (**NDHM**).[4] It also stated that an institution such as the NDHM which is undertaking significant reforms in health should have legal backing.

[4] The Blueprint proposed the creation stating that "*the Ministry of Health and Family Welfare has prioritised the utilisation of digital health to ensure effective service delivery and citizen empowerment so as to bring significant improvements in public health delivery.*"

A policy is not a substitute to a law passed by Parliament or by the state legislature. The Policy affects the fundamental right of privacy of individuals and the Supreme Court of India in the Puttaswamy case had clearly laid down that any action infringing the right to privacy has to pass a three-fold test (a) legality- existence of a law; (b) legitimate state aim; and (c) proportionality [5] International bodies have time and again recommended governments to come up with a robust data protection framework for health systems in order to uphold international human rights.[6]

A significantly large part of India's population lives in rural areas and is not digitally literate. This is true for even middle and lower income groups in urban areas. They are unaware of the concerns emanating from sharing data digitally, and the means to redress their grievances. Further, though the Policy does refer to transparency and accountability standards- however, policies are not justiciable in court (except if it is manifestly arbitrary) and therefore, any concerned individuals will have little or no recourse to seek the implementation of any of the standards prescribed in the Policy.

We recommend that prior to the rollout of the second version of the Policy, necessary and appropriate legislation be enacted-It should amongst other provisions clearly specify the accountability, transparency measures and penal provisions in case of negligence by the data fiduciary in processing the data of the data principal.

6. Definition of Sensitive Personal Data Needs to be in line with the Data Protection Bill

Clause 4(ee) of the Policy refers to Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules) for defining Sensitive Personal Data. It states that it will also include Official Identifiers (as defined by the Policy). As per Rule 3 of the SPDI Rules, Sensitive Personal Data means such personal information which consists of information relating to;—

(i) *password;*
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;

[5] Justice K. S. Puttaswamy (Retd) v Union of India, 2017) 10 SCC 1
[6] World Health Organisation, *Electronic Health Records: Manual for Developing Countries*, available at https://apps.who.int/iris/bitstream/handle/10665/207504/9290612177_eng.pdf?sequence=1&isAllowed=y (Last visited on May 20, 2022).

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

It is pertinent to note that while the final version of the earlier Policy (released on December 14, 2020) had also referred to the SPDI Rules for defining sensitive personal data, the draft version of the Policy released in August 2020 had provided for a more expansive definition of sensitive personal data[7], as provided for in the proposed Data Protection Bill. The rationale for referring to the SPDI rules to define sensitive personal data is unclear, especially since the proposed data protection bill is in the pipeline.

7. Need to make the Policy and its Implementation easily understandable to healthcare professionals

At the outset, we would like to state that the Policy and its wordings might be difficult for healthcare workers to understand, as it requires understanding not only earlier documents in the Policy as well as having a good understanding of national and international data protection principles. We suggest that the Policy wordings in the final document be in such a way that organisations that need to comply with the Policy can do so without additional help and thus incurring additional costs.

For the Policy to be an implementational success, there is a need to look at the existing infrastructure in this regard. The Economic Survey of 2021-2022 while looking at the importance of the healthcare sector, also highlighted that India has insufficient human resources for healthcare and that although aggregate human resources for health density in India is close to 23 for 10,000 population, there were still states that

[7] Clause 3(ee) defined sensitive personal data as "sensitive personal data" means such personal data, which may reveal or be related to, but shall
not be limited to,
(i) financial information such as bank account or credit card or debit card or other payment instrument details;
(ii) physical, physiological and mental health data;
(iii) sex life;
(iv) sexual orientation;
(v) medical records and history;
(vi) biometric data;
(vii) genetic data;
(viii) transgender status;
(ix) intersex status;
(x) caste or tribe; and
(xi) religious or political belief or affiliation.
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;

had varying numbers of healthcare workers.[8] Adding to the scarce healthcare workforce, Health Information Systems (HIS) in its present form are not equipped to handle, record, store and maintain swathes of data. For rural and even some urban hospitals with limited staff the implementation of this Policy can lead to them being overburdened and possibly dropout which could result in data gaps that could affect future policymaking.

While the Policy does mention training to be conducted, the burden is still on the data fiduciary to conduct them. We suggest that the NHA conduct free training sessions with organisations and bodies that will be collecting data on how to set up the infrastructure, how to digitise and how to record and maintain the data securely. A few initial training sessions will add more confidence and ensure that proper procedures are followed.

8. Reliance on digital infrastructure needs to be examined

While there is an understandable need for a digital economy, there is a need to look at the reality of internet coverage in India. The NITI Aayog Sustainable Development Goals (SDGs) India Index 2020-2021 report revealed that out of 55 of every 100 people had an internet connection,[9] although this is an improvement from previous years, there are 45 people out of 100 who would struggle with the digital-only approach. Similarly, the requirement of Health Information Exchanges to fill in details online does not take into consideration things like bad network, power shutdowns and internet shutdowns that can cause even places with internet access to be rendered ineffective. A history of poor internet access, long power outages, lack of technical support and public offices having insufficient backup measures for data storage and revival can lead to either delay in recording data or even the data going unrecorded. On the side of the data fiduciary, the need to have the Personal Health Records App to access and authorise medical data assumes that every individual has a smartphone. The reliance on an App can cause exclusion as was also seen when Aarogya Setu was released on only smartphones and was later made available on IVR.

We recommend that in the same way as the Policy provides the option to the Health Information Exchanges to keep physical and digital copies, the data fiduciary must have an option to opt for physical copies of the records and or digital copies.

---

[8] Healthcare takes centre stage, finally!, available at https://www.indiabudget.gov.in/budget2021-22/economicsurvey/doc/vol1chapter/echap05_vol1.pdf (Last visited on May 21, 2022).

[9] Revathi Krishnan, *More people in India got internet access in 2020 but fewer mobile connections: NITI Report*, June 10, 2021, available at https://theprint.in/india/more-people-in-india-got-internet-access-in-2020-but-fewer-mobile-connections-niti-report/675324/ (Last visited on May 21, 2022).

Additionally all mobile related services should have an IVR option that provides support in multiple languages, to help people understand and manage their data.

9. Need for more detailed privacy and security by design policy

The Privacy by design Policy mentioned in this Policy confirms to the 'Preventive not Remedial' principle, by prescribing the data fiduciaries to store the data of data principals in a federated and not in a centralised manner. While it is commendable that the Policy looks at privacy by design, it does not take into account some of the key principles, such as the 'Full Functionality – Positive-Sum, not Zero-Sum' principle. 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. For example, the Policy requires the data fiduciaries to make available a 'privacy by design' Policy on its website and details the various categories of information that such a Policy should contain. But, it lacks the specific directives on 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 such obligations could be under the 'privacy by design' Policy. Additionally, the Policy should include ways in which the interface and the ABDM system are made accessible to persons with disabilities; while the Policy does talk about privacy by design it also needs to look at the universal design, as well as international standards of privacy and security.

We reiterate our recommendations made to the 2020 draft Health Data Management Policy, that this 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 clearer detail, including aspects such as accommodating all legitimate interests and objectives in a positive-sum manner, without making unnecessary trade-offs, applying data minimisation and disclosure of breaches, using accepted standards and frameworks, which are amenable to external reviews and audits, and wherever possible, carrying out detailed privacy impact and risk assessments.[10] The Policy must also include the right of data principals to be informed of the breach and the compensation to be afforded to the data principal

[10] The Centre for Internet and Society, *Comments to National Digital Health Mission: Health Data Management Policy*, October 5, 2020, available at https://cis-india.org/internet-governance/blog/comments-to-national-digital-health-mission-health-data-management-policy (Last visited on May 21, 2022).

10. Need for a More Adequate Governance Mechanism

The lack of a legislative framework has led to a lack of clarity over the regulatory oversight of the ABDM which has either been established or proposed to be established. The Blueprint had recommended that the NDHM should include two separate arms, one for regulation and the other for operational maintenance, but under the Policy, there is no delineation of responsibilities and obligations in the NDHM. It is a monolithic entity overseeing both regulation as well as maintenance of the ecosystem.

The National Health Authority has been given the responsibility for the implementation of the ABDM. The NHA was established in 2019 to implement India's health insurance- Ayushman Bharat and is responsible for "*Working closely with Insurance Regulatory and Development Authority on development and implementation of Health Insurance Regulations targeting insurance companies, Third Party Administrators, hospitals and other stakeholders.*" Under the current framework, the NHA would have too many roles and a conflict of interest in managing the ABDM. With the Government being a large collector of health data, it is concerning that an independent regulatory/agency has not been established for regulating the health ecosystem in the country.

Further, the work of the NDHM is said to be dynamic. Therefore, the ABDM should consist of experts in areas of health care, technology etc. It is also important to ensure the independence of the ABDM-CEO

11. Concerns with Sharing of Data

As per Clause 28.1 of the Policy, '*any personal data processed by a data fiduciary may be shared with an HIU in response to a request made by such HIU for personal data pertaining to the data principal, only where consent of the data principal is obtained in accordance with Chapter III of this Policy.*" Further, as per Clause 29.1, data fiduciaries can make use of anonymised and de-identified data available "*for the purpose of facilitating health and clinical research, policy formulation.....and any other purpose that may be specified by the NHA.*" This provision raises the following important issues to consider and highlight:

A Health Information User (HIU) has been defined as entities that requests access to personal data of the data principal and considering the expansive scope of the

applicability of the Policy[11]- it appears that the data fiduciary can share the data with entities ranging from healthcare facilities, pharmaceutical companies to research organisations. Further, it is also concerning to note that while sharing of personal data has been permitted with such a wide range of entities; it does not specify or provide for any mechanism wherein the benefits that accrue from the sharing of such personal data is shared back with the concerned data principal(s). The concept of benefit sharing defined as the "*action of giving a portion of advantages/profits derived from the use of human genetic resources to the resource providers in order to achieve justice in exchange with particular emphasis on the clear provision of benefits to those who may lack reasonable access to resulting products and services is important in the case of personal data being used for clinical trials*"[12] has not been addressed in the Policy and no reference has been made to any other Policy document, legislation or guidelines addressing these concerns.

Another issue for consideration is whether the data fiduciaries can and will share personal data with insurance companies. Under the Digital Information Security in Healthcare Act (DISHA) Bill released by the Ministry of Health and Family Welfare in 2018, there was an explicit prohibition on sharing anonymised health data with insurance/pharmaceutical companies.[13] The Policy goes against the DISHA Bill on sharing of data with corporations. Insurance companies already have access to a significant amount of personal health information; and the use of such personal health information even in an anonymised condition leads to concerns about the harms from the usage of such data, especially to historically marginalised communities. The Policy should also specify purpose limitation as well as data minimisation.

The Policy needs to include stricter consent and accountability measures with respect to any transfer of data to, or processing of data, by HIUs.

12. Need Clarity on Role of Health Information Exchange & Consent Manager

The introduction of a separate type of consent manager called Health Information Exchange & Consent Manager creates more confusion than the inclusion of "consent manager" in the earlier version. The creation of a new class of consent managers with a modified definition still does not bring clarity on whether it is a person or an application. The Policy also does not provide clarity on who would be responsible for the consent manager, what oversight mechanisms are in place to ensure compliance with the Policy as well as the Data Protection Legislation. We recommend that the

[11] *Supra*, note 1.
[12] Schreoder D., *Benefit sharing: it's time for a definition*, Journal of Medicial Ethics, 33(4), (2007).
[13] Digital Information Security in Healthcare Act Bill 2018, Section 29(5).

constitution and governing of the consent manager be in line with the draft Data Protection Bill. Clause 3(11) of the Bill defines consent manager as "a data fiduciary which enables a data principal to give, withdraw, review and manage his consent through an accessible, transparent and interoperable platform;". The inclusion of the term "fiduciary" in the definition means that the consent manager also has the same responsibilities for handling data as a fiduciary, something which is absent in this Policy. The Data Protection Bill also requires that the consent manager be registered with the Data Protection Authority.

Another possible way would be to reintroduce the definition of consent manager from the draft Health Data Management Policy published in August 2020.[14]The Policy defined consent manager as "an entity or an individual, as the case may be, that interacts with the data principal and obtains consent from him/her for any 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;".

13. Opportunity to Withdraw Consent for Child on Attaining Majority or Person no Longer Being Incapacitated

While the Policy states that parents/guardians of a child can provide consent on their behalf the is silent on the status of the child's health records and the consent once they have attained the age of majority. We recommend that the Policy should include a provision which clarifies the rights the child will have towards their own data once they attain majority. This could be similar to the provisions in the Health Insurance Portability and Accountability Act (HIPAA) of the United States which 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. We also request that the Policy also make provisions for a person who was incapacitated at the time of giving consent to re-exercise all the rights granted by the Policy once they are no longer incapacitated. The Policy could take reference from the Health Insurance Portability and Accountability Act (HIPAA)[15] of the United States which states the rights of a person when they are no longer incapacitated or seriously ill.

---

[14] *National Digital Health Mission: Health Data Management Policy*, available at https://www.medianama.com/wp-content/uploads/National-Digital-Health-Mission-Health-Data-Management-Policy.pdf (Last visited on May 21, 2022).

[15] U.S. Department of Health & Human Services,. *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?*, September 21, 2020 available at https://www.hhs.gov/hipaa/for-professionals/faq/230/is-parent-rep-once-child-reaches-age-maturity/index.html (Last visited on May 21, 2022).

Additionally, Clause 12.3 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. This requirement 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. Similarly, the limited definition of family to biological family is exclusionary for LGTBQ+ persons since it ignores potential rejection by biological families and the reliance of LGTBQ+ on chosen families. We recommend that instead of requiring proof of identity or relationship the Policy could require the person to attest or verify that they are indeed who they represent themselves to be and legal recourse should be undertaken for misrepresentation.

14. Need for a Robust Grievance Redressal Mechanism

As per Clause 32.1 of the Policy, the data principal may approach the designated officer known as the Data Protection Officer to seek redressal of any queries regarding the processing of their personal data. However, the means to approach the Data Protection Officer are limited to electronic means- the data principal may approach the DPO in writing, through email or any other electronic means, as may be specified. Further, in the event the complaint is not resolved within 30 days, then the data principal may approach the ABDM-GRO (Clause 32.2) in writing or through an email ID or any other electronic means provided under the grievance portal of the ABDM website. Any non-electronic means to approach the DPO or the ABDM-GRO appears not to have been contemplated- this is concerning as internet access in India is far from ubiquitous with the latest estimate of internet subscribers in the country at 61.06 per cent[16] at the end of June 2021. It is also concerning that no time limit has been provided for the ABDM-GRO to address the complaint. We recommend that a maximum time period of 2 months be specified for the ABDM-GRO to address the complaint and the grievances.

We recommend that for an efficient and effective grievance redressal mechanism, the option to provide the complaint by physical mail and in-person should be permitted. Further, the redressal mechanism should also be specified through infographics and should be available in multiple regional languages. Additionally, the appellate mechanism and the relationship between such a mechanism with the proposed Data Protection Authority should be clearly specified.

[16] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators April – June, 2021*, October 21, 2021, available at https://www.trai.gov.in/sites/default/files/PIR_21102021_0.pdf (Last visited on May 21, 2022).

The current grievance redressal mechanism does not envisage a judicial mechanism that can serve as an appellate forum for grievance redressal and this does not adequately protect the right to privacy of the data principal. The right to privacy being a fundamental right protected under the Constitution of India, it is therefore imperative to have a judicial redressal mechanism to realise and protect such a right.

15. Concerns Regarding the Unique Health ID

As per Clause 19.1 of the Policy " *The participation of the data principal in the NDHE as set out under this Policy shall be on a voluntary basis only*". *An individual may link his/her health records with ABHA if he/she chooses to do so.*" It is interesting to note that the previous version of the policy had stated that "participation of an individual in the NDHE will be on a voluntary basis and where an individual chooses to participate, he/she will be issued a Health ID (as defined in this Policy) by the NDHM. The deletion of the highlighted section suggests if the individual chooses to participate in the NDHE- then the individual necessarily requires a Health ID.

Health IDs have de-facto been generated for beneficiaries who had registered using their Aadhaar[17] numbers across the country, without citizens having any choice in opting into the project. The beneficiaries who have had their Health IDs created through the vaccination process have not been informed about the creation of such an ID, or their right to opt-out of the digital health ecosystem. The beneficiaries are also not informed of their right to de-activate the UHID and reactivate it later if required.

The de-facto mandatory nature of Health IDs is concerning and raises alarm bells, as this is similar to the de-facto mandatory use of Aadhaar for accessing welfare services, which after the enactment of the Aadhaar Act also got legislative sanction. However, there have been several studies[18] which have revealed that a large number of Aadhaar holders face authentication problems while trying to access foodgrains through the Public Distribution System, and other state entitlements. Another study conducted in Andhra Pradesh[19] revealed that in 2015, more than half of the eligible beneficiaries

[17] This use of Aadhaar for identification and authentication purposes was made possible by virtue of a notification issued by the MoHFW on January 1, 2021, which officially permitted the Co-Win portal to use Aadhaar for registration of the Covid-19 beneficiaries

[18] Prashant Reddy, Aadhaar: *Amid the debate about privacy, the more pressing issue of exclusion has been forgotten*, March 29, 2017, available at https://scroll.in/article/833080/aadhaar-amid-the-hullabaloo-about-privacy-the-more-pressing-issue-of-exclusion-has-been-forgotten (Last visited on May 21, 2022).

[19] Hindustan Times, *Centre may allow Aadhaar authentication for social welfare schemes*, August 6, 2020, available at https://www.hindustantimes.com/india-news/centre-may-allow-aadhaar-authentication-for-social-welfare-schemes/story-0OcD8u2QceEptk2VRzWsyK.html (Last visited on May 21, 2022).

could not access the entitlements due to them under the social welfare programmes. Though the Policy clearly articulates that the absence of a Health ID should not lead to any denial of health services, the AADHAAR example has shown how voluntary linkage becomes mandatory.

16. Confidentiality and Consent

The Policy envisages a 'one-time consent'- taken at the first stage of processing of personal data. However, it does not contemplate consent to be taken by the data fiduciary from the data principal at each instance of data sharing and processing.

We recommend that the Policy be amended to provide for the data fiduciary to seek consent at each stage of processing of data, and consequently, it should also explicitly state that the data principal has the right to withdraw consent at any stage. The data principal should also have the right to correction and erasure of personal data
All provisions with respect to the non-consensual processing of personal data (such as in the "interest of public health") must be narrowly tailored and must contain explicit definitions of the data allowed to be processed under such exceptions. Further, Personal Data Processing Model Consent Form must explicitly mention that the collection of data is voluntary and refusal will not lead to exclusion from services

17. Exclusion errors and 'coercion-based inclusion

Situations such as exclusion from availing medical services due to compulsory use of Aadhaar must be avoided under the ABHA and EHRs project. Further, Aadhaar-based verification should be removed to ensure that issues related to privacy are at the very least partially addressed.