Comments on the Draft Health Data Management Policy

Centre for Health, Equity, Law and Policy

Centre for Mental Health, Law and Policy

1 Structure of the document

This document contains submissions to the *National Digital Health Mission: Health Data Management Policy* by the *Centre for Health, Equity, Law and Policy* (C-HELP), and the *Centre for Mental Health, Law and Policy* (CMHLP). The document is structured as follows: Section 2 contains submissions to the policy as a whole; and Section 3 contains submissions to each chapter of the policy.

2 Preliminary comments

Preliminary comments include submissions on the *National Digital Health Mission: Health Data Management Policy* (hereinafter referred to as "the Policy"), as a whole. The submissions are divided into three parts, including need for a law, implementation process and citizen engagement.

2.1 Need for a law

2.1.1 It is established law that any encroachment of fundamental rights and legal rights can only be provided by 'law'. Confidentiality and privacy of Medical/health data is a fundamental right under Article 21. Digitisation of health records and linkage with Unique Health Identifier (UHID) entail significant risks to confidentiality and privacy; and hence must have a legislative basis.

A. Under Article 73 of the Constitution, the Union Executive can make policies and executive directions even when there is no law. However, Legislation is required where the Constitution itself provides that the act can only be done by legislation. For instance,policies encroaching upon fundamental rights or other legal rights.[1] Article 21 states that no person shall be deprived of life or personal liberty except by a procedure established by law.

B. The Supreme Court in *Justice K. S. Puttaswamy (Retd) & Anr. Vs Union of India & Ors*[2] (hereinafter referred to as Puttaswamy judgement), firmly established the right to privacy of medical data as a fundamental right under the right to privacy flowing from Article 21 of the Constitution. The judgment laid down 'tests' against which privacy infringements will be evaluated going forward, namely: the measure must be a *"procedure established by law" aimed at a "legitimate goal"* , must be *"just, fair and reasonable" ,* "proportionate" to the objective sought to be achieved, and must have procedural guarantees to check against abuse of State or non-state actors interference.

C. The Supreme Court also observed that the growth of technology and digitisation has created new dangers for invasion of informational privacy, including profiling and surveillance by the State and non-state actors alike. Hence, it called for enactment of a comprehensive data protection law, codifying globally established privacy and data protection standards and rights of data subjects.

D. Absent data protection law, digitisation of health records, creation of Electronic Health Records (EHRs) on a permanent basis; creation of UHID and linking it with digital health records and EHRs, data sharing with and between government and private entities, across different digital technology products, services and applications, have huge ramifications for fundamental rights to informed consent, confidentiality and privacy of medical records.

E. UHIDs are described as 'privacy-invasive tools of eHealth'as it has the potential to link data from EHRs with other data sources.[3] The use of Aadhaar to create a UHID, can be linked with other personal information, creating a bearing surface for surveillance by State and for profiling for commercial profits by private entities. There are many documented examples worldwide of abuse of the

[1] State of M.P. v Bharat A. 1967 SC 1170 paras 5-
[2] ((2017) 10 SCC 1)
[3] Soenens, E., Leys, M. (eds.): eHealth identity management in several types of welfare states in Europe. FIDIS Deliverable D4.11 (2008). Available at: www.FIDIS-project.eu

personally identifiable information stored in databases.[4] Further, breach of sensitive medical data can cause embarrassment, humiliation, loss of reputation and stigmatization. Access by third parties, could lead to discrimination against individuals for instance, denial of insurance and discrimination in employment.

F. The Policy and accompanying guidelines lack statutory force and cannot enforce data protection and privacy standards. The Policy itself states that its objective is "to encourage stakeholders and ecosystem partners to adopt the data protection principles set out in this Policy" [See para 3, page 2).

G. Therefore, it is imperative that digitization of medical records and UHIDs must have a clear legislative basis. However, the NDHM pilot project has been rolled out, not just without legislative authority but even before finalisation of the instant Policy. According to news reports, over one lakh UHIDs have been created by citizens in India within one month of the launch of government's NDHM.[5] As components of NDHM, including EHRs and UHIDs gravely imperil fundamental rights to privacy, it must be accompanied by a law and its implementation without legislative authority is unconstitutional.

2.1.2 The World Health organization (WHO) also calls upon member states to implement digital health accompanied by strong data protection laws

A. The World Health Assembly Resolution on Digital Health, passed in May 2018, acknowledges the potential of health technology to enhance health service capabilities.[6] However, it also calls upon member states to develop legislation around issues such as data access, sharing, consent, security, privacy and inclusivity consistent with international human rights obligations.

B. In its Manual for developing countries, WHO states that in order to implement a successful transformation from paper to digital records, which harnesses its benefits and minimizes the risks and harms associated with it, governments must do the groundwork and ensure both: a) health system preparedness- improve healthcare documentation to ensure accuracy of data, facilitate infrastructural capabilities, fulfill human resources and training requirements for data analysis

[4] UNAIDS: Considerations and Guidance for countries adopting national health identifiers. Available at: https://www.unaids.org/sites/default/files/media_asset/JC2640_nationalhealthidentifiers_en.pdf

[5]https://www.livemint.com/news/india/unique-health-ids-under-ndhm-program-will-never-be-mandatory-harsh-vardhan-11600010335236.html

[6] World Health Assembly Resolution on Digital health. 26 May 2018. Available at: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf

and translation of data into actual health action, strengthen quality control etc.; and b) a comprehensive data protection law and regulatory capacities, which regulates all processes related to data, protects rights to consent, confidentiality and privacy, and safeguards individual's health data from unauthorized access, abuse and theft.[7]

2.1.3 The existing laws are not adequate to protect rights to consent, confidentiality, privacy and security of health data/sensitive health data

The Policy mentions at several places that the implementation will be as per the existing laws and any further law or regulation that may be laid down by National Health Authority under NDHM. With respect to existing law, it is submitted that it is inadequate to ensure adequate privacy and protection of personal medical data. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("2011 Rules") framed under Section 43A of the Information Technology Act, 2000 ("IT Act") have several limitations – a) all obligations apply only to bodies corporate; b) The Rules do not codify the established privacy and data protection standards; c) The Rules do not prescribe criminal penalties for a breach of personal data and only cover accidental or negligent breach and not intentional ones.

2.1.4 The Policy and accompanying guidelines cannot be contrary to or override existing statutory provisions

A. Government cannot amend or supersede statutory rules by executive action or administrative instructions.[8] Any order, notification, direction or notification issued in exercise of the executive power of the state which is contrary to any other statutory provision, is without jurisdiction and is a nullity.[9] However some provisions of the Policy, read together with accompanying documents issued under the NDHM, contravene and are otherwise contrary to existing laws:
    - The Policy mentions that the use of Aadhaar will be voluntary for creation of a unique health Id. However, the Frequently Asked Questions (FAQs) on NDHM website state that the use of Aadhaar is mandatory for creation of health practitioner Id as well as health facility Id. This is a clear

[7] 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
[8] Jagjit Singh v State of Punjab AIR (1978)2 SCC 196; Mahadeo Bhau Khilare v. State of Maharashtra SCC (2007) 5 SCC 437
[9] State of Sikkim v Dorjee Tshering Bhutia 1991 AIR 1933

violation of the Aadhaar Act post Puttaswamy judgement (for details refer to note at Annexure 1).

- The provisions in the Policy on 'storage of medical data' and 'right to erasure' read with NDHM Strategy Overview (which states that care providers have to store medical records digitally indefinitely) exceed the minimum data storage requirements under: The Indian Medical Council Act, 1956; and The Pre Conception and Pre Natal Diagnostic Techniques Act, 1994; and The Medical Termination of Pregnancy Act. (for details refer to note at Annexure 1).

2.2 Implementation process

2.2.1 A nationwide Unique Health ID (UHID) system is large, complex, involves significant financial implications and poses risks to the fundamental right to privacy of individual citizens. The complexity of the system is illustrated under Clause 2.2.1 of the Blueprint, which proposes a decentralised architecture where digital health data will be held at the centre, state and facility level. Hence, the UHID system entails a detailed plan for implementation, so as to ensure its efficiency, effectiveness, economy and equity.

2.2.2 The implementation plan should involve critical analysis of existing infrastructure and state capacity; enacting a supporting law and regulatory governance standards under the law; plan for capacity building; assessment of financial implications and budgetary approvals; conducting pilot studies and incorporating feedback into the process; and finally actual implementation of the system.

2.2.3 The Blueprint recognises the aforementioned aspects as building blocks for UHID in the Blueprint: (a) standardisation of collection and storage of medical data to ensure accurate linking of individuals, medical records and consent for access (Clause 2.4(ii)(a)); (b) technology standards, particularly anonymisation and consent management (Table 2); (c) governance standards for consent management, data interoperability, privacy and security, and patient safety and data quality (Clauses 3.3-3.6); (d) financing model requiring budgetary support from the Government of India, at least in the earlier years (Clause 4.10); and (e) need for capacity building (Clause 4.10). Further, Table 5.1 of the Blueprint lays out an action plan, under which the UHID system should be established in the second year of implementation.

2.2.4 Media reports suggest that the UHID system is already underway. Recently, Dr. Indu Bhushan announced that 1 lakh Health IDs have been created across Indian union

territories, and the National Health Authority has launched the NDHM Sandbox. This indicates that the UHID system is being implemented without:

(a) a law;
(b) the Policy being finalised and approved;
(c) clarity on crucial protocols on standardisation of medical data, processes and systems for anonymisation and consent management and governance standards; and
(d) detailed assessment of financial implications, as well as budgetary support for implementation.

2.2.5 The Policy itself leaves standards and processes, essential for the governance and implementation of UHID, to be formulated at a later stage. This includes the governance structure, framework for consent management, processes for issuing a unique health ID, technical processes and anonymisation protocols. The Policy is also silent on standardisation processes.

2.2.6 Further, the UHID system is being implemented in contravention of the Action Plan laid out under the Blueprint. The Action Plan envisages the UHID system to be established in the second year. The Plan envisages development of federated enterprise architecture, designing building blocks and standards, security and privacy policies and consent management framework, prior to the implementation of the UHID system. In reality, the UHID system is being implemented before compliance of any of these prerequisites.

2.2.7 In light of this, keeping in mind the complexity of the UHID system, its implementation should take place in a staggered manner, following the Action Plan as laid under the Blueprint.

2.3 Active citizen engagement

2.3.1 The Policy does not envisage active citizen engagement in the development of the UHID system.

2.3.2 We feel that effective public participation in the development of the UHID System is essential to ensure that the system and policies are responsive to actual requirements of patients, health care workers, health facilities and health systems. It will also help to check and improve the analysis of the governing authority, and the quality of information used.

2.3.3 In light of this, we suggest that details of the process to be followed for carrying out consultations and receiving public comments on proposed changes or additions to the Policy and accompanying processes, should be laid down in the Policy itself.

2.3.4 The public consultation process should be carried out in two stages: (a) issuance of proposed changes or additions to the Policy and related processes, to the public; and (b) process for responding to public comments and finalising the proposed changes.

2.3.4 In the first stage, the document containing the proposal should be accompanied with a statement of the problem sought to be addressed, and a cost benefit analysis. The proposal should be put out for public comments for at least 30 days.

2.3.5 In the second stage, all public comments along with a reasoned response to the comments, and a review of the proposal based on the public comments, should be published.

3 Specific comments

Notwithstanding our preceding submission that the Policy cannot be approved and enforced in the absence of a governing law, this section contains our comments on each chapter of the Policy (in chronological order).

3.1 Purpose

3.1.1 Clause 1 states that the Policy is the first step towards ensuring “Security and privacy by design”, the guiding principle of NDHM. In doing so, the Policy sets out minimum standards of data privacy protection.

3.1.2 At the outset, the principle of “privacy and security by design” necessitates adoption of state of the art standards and not minimum standards of privacy and security.[10]

3.1.3 It is necessary to adopt standards for privacy and data protection both by *design* and by *default*. Privacy by design emphasises the need to be proactive in considering the privacy requirements from the design phase throughout the entire data lifecycle. It does not wait for privacy risks to materialise, it aims to prevent them.

[10] Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*. Available at: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

3.1.4 Privacy by default involves ensuring that personal data is automatically protected in any given IT system or business practice. The individual does not bear the burden of striving for protection when using a service or a product but automatically enjoys the fundamental right to privacy and protection of personal data. Technology and product providers when developing, designing, selecting and using applications, services and products that are based on the processing of personal data, should be able to demonstrate compliance with the principle of privacy by default.

3.1.5 As an example, data protection by design and by default is not only a recommended good practice, but a legal and fully enforceable obligation under Article 25 of EU General Data Protection Regulation (GDPR) 2016. The principle is binding on technology designers, producers and data controllers, who are obligated to take technological data protection into account right from the planning stage of information-technological procedures and systems

3.1.6 In light of this, we suggest that “privacy by design” under Clause 1 of the Policy should be replaced with “privacy by design and default”.

3.2 Applicability

3.2.1 Clause 2(b): Does ‘Healthcare workers’ in this clause include community health workers, clinical psychologists, psychiatric social workers, psychiatric nurses, counsellors, and rehabilitation professionals? If no, then the definition of healthcare workers should be expanded to include the above mentioned categories.

3.2.2 Clause 2(c): Will governing bodies under the MoHFW under this clause include the Central and State Mental Health Authorities, State Mental Health Review Boards, and Central and State Disability Advisory Boards? If no, then they too should be included.

3.3 Objectives

3.3.1 The draft Policy, with its primary focus on digitisation of health and medical records, would lead to the exclusion of or unfair treatment of large parts of the Indian population, many of whom are not digitally literate, or reside in parts of the country which lack the required IT infrastructure. The policy should include as an objective that it will develop alternative forms and channels of communication as a means of providing and seeking information and consent with respect to people who do not have access to digital infrastructure or are not conversant and comfortable with electronic forms of communication.

3.3.2 Clause 3(c) of the Policy provides for the creation of a system of digital medical health records based on consent and in compliance with international technology and privacy standards. The Policy must mention as an objective: that the NDHM will publish periodic reports demonstrating the compliance of standards that it seeks to implement with the principles of privacy and data protection by design and default,

3.3.3 Clause 3(f) of the Policy seeks to encourage stakeholders and ecosystem partners to adopt the data protection principles as set out in the Policy.

3.3.3 Clause 3 of the Policy should also obligate NDHM to regularly assess, improve, monitor and publish the conditions and preparedness of health systems to support UHID, particularly with regard to improving information systems, strengthening data recording and reporting, training and capacity building of human resources, and enhancing capacity for data analysis. This will ensure that NDHM serves patient privacy and safety, and better health outcomes.

3.4 Definitions

3.4.1 Clause 4(a) of the Policy defines anonymization. As per the definition the data principal "cannot be identified through any means reasonably likely to be used to identify such data principal." This leaves open the possibility of re-identification. In contrast, the Data Protection Bill 2019 clearly states "transforming or converting personal data to a form in which a data principal cannot be identified, which demonstrably meets the standards of irreversibility." Hence, the definition should be modified to meet the same standard as set out in the Data Protection Bill 2019.

3.4.2 Clause 4 (e) and (f): The definitions of "consent artifacts" and "consent managers" needs to be made clearer, and should be included in Section 2 of the Policy.

3.4.3 The definition of 'consent' in Clause 4(d), should be replaced with the definition of "informed consent" under Mental Healthcare Act, 2017.

3.4.4 Clause 4(h) defines data fiduciary. The definition has been taken from the Data Protection Bill 2019 and is broad as the Bill is an omnibus law covering various sectors. For the purpose of the Policy, which is specific to the health sector, the definition should restrict the number of entities who can be data fiduciaries. In particular, 'health information users' may include several entities who may not be engaged in the provision of health services. As an example, the DISHA Bill, 2017 specified that digital health data

may be generated, collected, stored, and transmitted by a clinical establishment or health information exchange, or other entity for providing direct treatment to the person, and coordination between hospitals for effective treatment of the person concerned.

3.4.5 Clause 4(j) defines data processor. It is submitted that The criteria and process based on which a company will be identified as a 'data processor' should be mentioned in the policy, as well as whether these companies will be public or private entities, and for what purposes they can process data.

3.4.6 Clause 4(p)**:** Does the definition of 'Health Facilities' also include rehabilitation centres and facilities for persons with mental illnesses and/or disabilities? If no, then the definition should be expanded to include these.

3.4.7 Clause 4(cc) of the Policy defines pseudonymisation. The definition may be replaced with the definition of pseudonymisation as provided under GDPR.

3.4.8 Clause 4(ee) of the Policy defines sensitive personal data is incomplete. The definition should also include: details on family members, information on personal relationships/ life and personal communications, Health ID, personal health identifier, communications content and metadata, as this information reveals particularly sensitive information. Further, the term "transgender status" mentioned under this definition should be replaced with "gender status".

3.4.9 Clause 4 of the Policy should include a definition of profiling, i.e. any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. The definition should be connected with the right to decline being subjected to a decision solely based on automated processing.

3.5 Applicable Law and Governance structure

3.5.1 Under Clause 6, the governance structure for the National Digital Health Ecosystem (NDHE), as specified by the National Health Authority (NHA), will be responsible for implementing the Policy. The Blueprint states that the National Digital Health Mission (NDHM) will promote and facilitate the evolution of NDHE. Specifically, Clause 4.13 of the Blueprint states that *Unique Health ID* will be one of the key services provided by the NDHM. It follows that NDHM will be the governing authority under Clause 6 of the Policy. Clauses 4.5 and 4.6 of the Blueprint provides that NDHM will be

a government owned body comprising two separate arms: (a) governing council and board of directors responsible for policy formulation and regulation; and (b) CEO and operations team responsible for implementation of the policies. In addition to this, Clause 6 of the Policy provides that the institutional framework will include the NDHM Data Protection Officer (NDHM-DPO), who will serve as an escalation point for decision making on matters concerning data privacy and governance.The CEO and the NDHM-DPO will be government officers.

3.5.2 At the outset, a regulator must be well-structured, composed of experts from the relevant field, remain independent from the pressures of the government and should be appointed in a fair and transparent manner.

3.5.3 The Blueprint lays out the principles and broad structure of NDHM providing clear separation of legislative and executive functions. However, neither the Blueprint nor the Policy specify the size, composition, selection process, tenure, powers, functions, terms of removal, finance and the accountability framework for various entities constituting NDHM. In contrast, Schedule 18 of the Health and Social Care Act 2012 and the Public Governance, Performance and Accountability (Establishment of the Australian Digital Health Agency) Rule 2016 clearly lay out these details in respect of NHS-Digital and Australian Digital Health Agency in the UK and Australia, respectively. In the absence of aforementioned details, there is no clarity on the terms of constitution and functioning of various entities of NDHM.

3.5.4 The Policy provides for the collection, storage, protection and sharing of personal and sensitive health data of individuals. In doing so, the NDHM should balance between establishing and maintaining the digital health records ecosystem in an efficient and cost-effective manner, while ensuring protection and privacy of individual health data. The task is complex and requires expertise in various fields, including health care, clinical safety and governance, health informatics, consumer health advocacy, technology, privacy and cyber security. It is important that the NDHM governance structure reflects this. As an example, Section 19 of Public Governance, Performance and Accountability (Establishment of the Australian Digital Health Agency) Rule 2016 lays out the eligibility criteria, providing for a diverse pool of expertise, for appointment to the Australian Digital Health Agency.

3.5.5 Clause 6 of the Policy and Clause 4.6 of the Blueprint states that NDHM members, including the CEO and NDHM-DPO, will be government officers. The two members are responsible for the implementation of NDHM and the Policy. Government officers holding these positions may expose the regulator to pressures from the government and compromise its independence. As an example, the boards of

NHS-Digital and Australian Digital Health Agency, while responsible to the parliament, do not have any government representation.

3.5.6 Clause 6 of the Policy and Clause 4 of the Blueprint indicates that NDHM is the governance authority. Clause 4.6 of the Blueprint proposes that the governing council and board of directors under the NDHM will be responsible for policy formulation and regulation. This implies that the rule-making power under the Policy should lie with the NDHM governing council and board of directors. In contrast to the proposed institutional framework, the rule-making power under the Policy is with the NHA (See Clauses 6, 9.3, 15.2, 15.7, 17.3, 18.3, 20.3, 21.2, 23.1, 23.2, 29.1, 29.2, 29.4 and 33.2).

3.5.7 Media reports suggest that implementation of the Policy is underway. Recently, Dr. Indu Bhushan announced that 1 lakh Health IDs have been created across Indian union territories, and the National Health Authority has launched the NDHM Sandbox. Implementing the Policy in absence of a governing authority poses serious risks to the protection and privacy of individual health data.

3.5.8 In light of this, we suggest the following modifications to the governance structure proposed under Clause 4 of the Blueprint and Clause 6 of the Policy:

(a) Specify the terms of constitution and functioning of NDHM in clear terms. This should include size, composition, procedure for selection, tenure and terms of removal of members of NDHM, as well as powers, functions, financing and reporting framework for NDHM entities.
(b) Specify the skills, experience and knowledge required for appointment of members of NDHM, with the objective of including expertise from relevant fields.
(c) Government officers should not hold any executive or non-executive positions in the NDHM. The government may nominate government officers as ex-officio members, to represent the perspectives of the government in the functioning of NDHM.
(d) Rule-making powers under Clauses 6, 9.3, 15.2, 15.7, 17.3, 18.3, 20.3, 21.2, 23.1, 23.2, 29.1, 29.4 and 33.2 of the Policy should be with the governing council and the board of directors of NDHM.
(e) No aspect of the Policy should be implemented prior to establishing the NDHM.

3.6 Consent Framework

3.6.1 The Policy does not expressly provide for the principle of purpose limitation and prohibit use of personal data for commercial purposes. We recommend including the following provision as provided under the DISHA Bill, 2017:

> "Digital health data, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may be specified by the Central Government."

3.6.2 Under Clause 9.1 of the Policy, data fiduciaries can collect or process personal or sensitive personal data only with the consent of the data principal. We recommend that: (a) the definition of data fiduciary should be limited to entities who are engaged in health service delivery, or clinical or public health research, as also recommended under Section 3.4.2 of this document; and (b) the collection and processing of data should be expressly limited to the purposes specified in the Policy, and never for the purposes which expressly prohibited under the Policy.

3.6.3 Clause 9.2 (b) of the Policy states that consent from the data principal will be valid only if it is "*informed, having regard to whether the data principal has been provided with the necessary information by way of notice, as set out in paragraph 10 of this Policy, the scope of consent in respect of the purpose of processing.*" Further, Clause 10.4 states that the "*privacy notice shall be clear, concise and easily comprehensible to a reasonable person and shall be available in as many languages in which the services of the data fiduciary are intended to be provided.*" However, it is not sufficient that necessary information is provided in an easily comprehensible manner. It is essential that the person must understand the purpose, benefits and potential risks of a health-related process. Key guidance in ISO/TS 17975:2015 states that,

> *"While subjects of care are normally content for information to be collected and used in order to provide their health care, it is still important that reasonable efforts be made to ensure that they understand how their information is to be used to support these activities and how it might be used in the future."*

While recognising that the consent process can be burdensome ISO/TS 17975:2015 emphasizes the import of undertaking it in a manner that makes the substance of it fully understood:

> "*It is acknowledged that undertaking the consent process can be difficult, either because the subject of care's age, disabilities or circumstances have prevented them from becoming informed about the likely uses of the information, or because they cannot effectively communicate their decision. In the former case, extra care will ensure that information is*

provided in a suitable format or language that is accessible to the subject of care and will also ensure that it has been understood."

In light of this, we recommend that Clauses 9.2 (b) and 10.4 of the Policy must incorporate sufficient requirements that informed consent is not characterised by a privacy notice that is simply easily comprehensible, but that it is obtained after ensuring that the data principal gives consent based on a proper understanding of the substance for which consent is being sought.

3.6.4 Clause 9.2 (e) of the Policy suffers from lack of clarity. It is not clear how or why the capacity to withdraw consent is qualified by "having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given."

3.6.5 Clause 12 of the Policy is cognisant of the needs of minors. However, some gaps remain and need to be dealt with. As an example, Clause 12.4 of the Policy states that "*Where the data fiduciary is processing the personal or sensitive personal data of a child, then they shall not process such personal or sensitive personal data in a manner that is likely to cause harm to the child*", it is unclear how and whether this would apply in situations where the data principal is a child who has *experienced sexual assault*.Such a child would be averse to having this sensitive personal data shared with others, particularly with parents or guardians. Their needs must be accounted for while devising consent modalities in relation to their health.

Further, the policy should *define 'best interests of the child'* in terms of the *Juvenile Justice Act 2015*: *"the basis for any decision taken regarding the child, to ensure fulfilment of his basic rights and needs, identity, social well-being and physical, emotional and intellectual development." Finally,* clarity needs to be provided on the event of a *child attaining majority*, and fresh consent that will require to be taken at such time. The following can be inserted: "Upon attaining majority, the minor shall have a right to withdraw or modify his/her consent for the collection, storage, transmission of their personal health data"

The Provisions of this Policy should also be in compliance with Section 23 of the Protection of Children from Sexual Offences Act, 2012, and it should be ensured that no sensitive personal information about a child is disclosed by the media or to the media by any third party or entity within the NDHE.

3.6.6 Clause 13. As per Section 14 of the Mental Healthcare Act, 2017, a person with mental illness may appoint a Nominated Representative for making decisions on the person's behalf. With regards to obtaining data and consent from data principles who

have mental illness and do not have capacity to make decisions, for the purpose of this policy, Nominated Representatives appointed as per the provision of the MHCA should be consulted instead of the “nominee”. The provisions under Section 13 of this draft policy should be revised to include Nominated Representatives, as mandated under the MHCA.

3.6.7 Clause 14 of the Policy sets out the rights of data principles. First, the rights of data principals/owners are not spelt out as affirmative rights, but are presented more in the nature of what the data principal/owner can ‘request’. Second, not all the rights, which are part of globally accepted and codified rights are included. Third, the Policy must ensure the softwares and technology standards deployed are demonstrated to be able to support the full realisation of these rights. The Policy must unequivocally state that the following are the rights of the data principals/owners: right to access, right to object, right to erasure, right to rectification, right to information, right to explanation and right to portability.

3.6.8 Under Clause 14.1(a) of the Policy, the data principal should have the right to receive the following information, in addition to the ones mentioned already – information as to what category of personal data, whether identifiable or not, have been shared with which entities, at what dates and times, and for what purposes.

3.6.9 Clause 14.1(b)(i) of the Policy related to the correction of data. Clarity is required whether the data principal can correct or complete or update any data, only in their personal health records (PHRs) kept in the digital health locker, or also in the EMRs or EHRs.

3.6.10 Clause 14.1(b)(ii) of the Policy relates to the erasure of data in certain circumstances. We recommend as follows:

(a) The first bullet states “if the storage of the personal data violates any of the data protection principles or the purpose for which it was originally collected has been satisfied”. It does not clarify that the exercise of this right will depend on the satisfaction of which person, entity or authority?
(b) The third bullet states that “if the storage of the personal data for a certain period of time is mandated by law, it cannot be erased”. However, it does not state positively that there shall be a right to have medical records erased after the end of the statutory time period, under different law, like the MCI Ethics Regulation, which mandates data be stored for 3 years. Further, the MTP Act, 1971 expressly mandates that the register of women who have undergone MTP must be maintained as a highly secret document and must be destroyed on the expiry

of a period of five years. Hence, the Policy must unequivocally state that after the expiry of statutory time periods, the medical data can be erased upon request, and if an existing act mandates destruction, then it must be automatically done, without awaiting a request for it. Further, it is recommended that highly sensitive data (like pertaining to MTP or sexual assault or domestic violence or a suicide attempt), may not be maintained in EMRs or EHRs (unless specifically consented to upon presentation of the option) as they are highly vulnerable to data breach.

(c) The fourth bullet states that *"personal data can be blocked and restricted, rather than erased … if the data principal disputes that the personal data is correct, and it cannot be ascertained whether they are correct or incorrect. "*It is submitted that if the Data Principal claims that personal data is incorrect and if the data fiduciary or others, cannot establish the falseness of her claim, then in light of the fact that 'ownership' and 'control' vests with the data principal, the data should be erased. Considering that digitisation of medical records is done with the main purpose of improving provision of direct care to the data principal, then would it be safe or professionally accepted to act on personal data, which the data principal claims to be incorrect. Further, if the objective of blocking or restricting it to prevent its processing or further use, then there is no reason why it should not be deleted instead.

(d) The fifth bullet states*"Where erasure is not possible without disproportionate effort due to the specific type of storage, over-writing, anonymisation or other method(s) of removal of the personal data from live systems can be used"* The Policy needs to provide more explanation on this clause. It is submitted that the right to erasure is a very important right and it must be ensured that softwares that are used for storing etc. support this right rather than impeding it.

3.6.11 Clause 14.1(c) of the Policy on right to 'restrict or object to disclose' states *"subject to applicable law, the data principal can restrict or object to the disclosure of their personal data by the data fiduciary."* The Policy must list down which laws and statutory provisions mandate the sharing of personal data, without consent of the data principal. Information on this must also form part of the protocol for informed consent.

3.6.12 Clause 14.1(d) of the Policy on data portability uses vague and evasive language such as, "as may be applicable" and "to the extent technically feasible". It is not clear as to why data fiduciaries and other entities who voluntarily join the NDHE and process personal data in digital form, will not at the very minimum be able to provide to the data principal, a digital copy of their personal data. Therefore the clause must be suitably amended to at least mandate that. It is understood that achieving interoperability is a big

challenge and progress on it will be gradual. However, it must be ensured that health facilities and other data fiduciaries adopt softwares and technology that allow interoperability, and the use of vague language does not do that. Infact, this is one of the reasons why it is recommended that the government must continuously strive to improve the technology infrastructure, particularly in the public health system, at least to some minimum benchmark level before rolling out NDHM.

3.6.13 Clause 14.2(a) of the Policy states that *"All requests under paragraph 14.1 above will be made by the data principal in writing, through e- mail or any other electronic means to the designated officer of the data fiduciary either directly or indirectly through a consent manager."* It is submitted that in light of the real issue of digital divide and digital illiteracy, the Policy must lay down a standardised format for making the requests, both in electronic form and on paper; must provide the procedure to be followed by the consent manager, designated officer and or data fiduciary upon receiving of a request.

3.6.14 Under Clause 14.2(b) of the Policy, the procedure for how data fiduciary will acknowledge the receipt of the request must be laid down and within how many days of receipt. Further, it must be clearly laid down the time lines within which the request will be addressed.

3.6.15 Under Clause 14.2(c) of the Policy, the 'necessary steps' that data fiduciary will take and the 'manner in which they will notify' all relevant entities, of making any alterations etc.

3.6.16 Under Clause 14.2 (d) of the Policy, the order by the data fiduciary denying the request of the data principal, must fulfill the criteria of a 'reasoned order'. The Policy must clarify what use is personal data subjected to if it is marked 'disputed'. Finally, the data fiduciary must also inform the data principal if their request has been accepted and what actions have been taken thereon.

3.6.17 Under Clause 14.2(e) of the Policy, the manner of taking consent for sharing personal data with relatives, after one's death, must be spelled out and must be recorded.

3.6.18 Clause 14.2 (f) of the Policy states that with reference to para 14.1 (requests), data fiduciary will not impose restrictions on the method and channel of raising requests. Instead, the Policy must impose a positive obligation on the data fiduciary that

they must have in place diverse channels and methods of raising requests, in order to provide access to all people (in context of digital divide and digital illiteracy). However, all these different channels and methods must have a governance structure, in terms of documentation and record keeping.

3.6.19 Under Clause 14.2(g) of the Policy, the data fiduciary must not only maintain records of all requests made, but also record the timelines and final decision made.

3.6.20 Clause 26.4 of the Policy states that data fiduciaries "*will give data principals a choice to opt-in/opt out of the NDHE.*" This is unclear and the policy needs to be categorical in its deployment of opt-in or opt-out to enroll data principals. Using both is untenable. Given the critical nature of health data management, opt-in should be the basis for informed consent under the policy, as well as the method employed to make data principals partners in the process.

3.7 ID Policy

3.7.1 Comments on the issue of Health Id have been made in preliminary submissions on the need for a law and may be read as part of the comments for this section as well. Further, it has been highlighted in the preliminary submission (para 2.1.4) that the FAQs on NDHM website state that Aadhaar is mandatory for creation of health practitioner and health facility Id. (See details at Annexure 1). This is violative of the Aadhaar Act post the ***Puttaswamy*** judgement and hence any mandatory requirement of Aadhaar must be stopped immediately and the FAQs must be modified accordingly.

In light of the comments referred to above, the Recommendations on Health Ids are:

3.7.2 As discussed in the UHID comments in the preliminary section, UHIDs and its linkage with personal health records are deeply intrusive and its rollout absent data protection and health sector specific laws/rules (In fact, even before the finalisation of this Policy) is unconstitutional. Hence, the rollout should be stopped and deferred till appropriate laws are enacted.

3.7.3 Meanwhile, the government should issue a 'proof of concept' and engage in public debate on its feasibility (technological, ethical and legal considerations)

3.7.4 The Policy must provide information regarding the structure of the Health Id (to assess whether it has any personally identifiable information); the means through which it is generated (which is left to be developed by NHA); the mechanism of how it gets

created to ensure that it is 'unique' (because that is the whole justification of the exercise); or what technology will be used to ensure privacy and security of health Id and keep it de-linked from Aadhaar number (where it is used for creation of health Id). As the Policy is silent on the above critical information, it is impossible to comment on those aspects. Hence, at the minimum the following recommendations are submitted:

- The design of the patient identifier should be content free- no information about the sex, age or place of birth of the patient - and irreversible to guarantee anonymity.
- The minimum security standards require that there should be a differentiation between the identification function and access control function(for audit trails and /or preventive actions).[11]
- Aadhaar must not be used as a direct health/patient identifier and linked with EMRs and EHRs. However, if it is used on a purely voluntary basis, as the basis for the creation of a Health Id, it should only be done if irreversibility and thus anonymity is guaranteed. As some experts have suggested, this could be ensured by using a 'double hashing method'(a first coding from Aadhaar to health identification number (for health portal) and a second one (for data processing shelter).[12] This way the privacy risks can be minimized.

3.7.5 The Policy must categorically state that when people are asked for Id cards to form the basis for creation of health id, they should be specifically informed that they can give any Id card and not only Aadhaar number. No direct or indirect influence should be applied on persons to provide their Aadhaar number, so that they can exercise their choice independently.

3.7.6 A specific and additional notice and consent format should be made and used for taking informed consent of persons for creation of a Health Id and taking consent with respect to which identity card/number they would like to use for creation of Health Id. It is not quite clear if one could give consent for processing of personal records for EMRs

[11]Els Soenens: Identity Management Systems in Healthcare: The Issue of Patient Identifiers. The Future of Identity in the Information Society, 2009, Volume 298. Available at: https://link.springer.com/chapter/10.1007/978-3-642-03315-5_4

[12] Quantin, C. et al.: Building Application-Related Patient Identifiers: What Solution for a European Country. International Journal of Telemedicine and Applications, vol. 2008, article ID 678302, 5 pages (2008). Available at: http://www.hindawi.com/GetArticle.aspx?doi=10.1155/2008/678302&e=cta

and EHRs, without giving consent for creation of a unique health Id or whether they must go hand in hand.

3.7.7 People who don't want to join the NDHE/get a Health Id should not be denied access to health services, be it in private or public health facilities. Persons who are not a part of this system shall continue to enjoy access to the healthcare system in exactly the same manner as they are doing now. Participation in the digital health ecosystem shall be completely optional and shall never be made mandatory for individuals.

3.8 Principles for processing of personal data

3.8.1 At the outset, Chapter V repeatedly mentions "conformity to requirements laid down by law", which implies that personal data collection and processing should not be done till such a law is enacted.

3.8.2 After Clause 26.1 of the Policy, all privacy and data protection standards must be listed down with clarity and without mixing them up or bringing in other elements. This should be followed up with specific measures related to accountability, transparency and demonstrating compliance with the data protection and privacy standards.

3.8.3 Analyzed critically the creation of EHRs - as a longitudinal complete health record from cradle to grave- militates against principles related to data minimisation, purpose limitation and storage limitation as healthcare organizations encourages collecting more and more amount of data and to save it for longer period of time for the purpose of detailed analysis, mining and predictions.

3.8.4 Replace Clause 26 with "Privacy and data protection standards to be followed by data fiduciaries and producers of technology products, services and applications"

3.8.5 Replace Clause 26.1 with the following: *"data fiduciaries will be accountable for complying with below mentioned privacy and data protection standards, implementing technical and organizational measures, selection of technology products, services and applications that demonstrate compliance to 'privacy by design', to ensure that rights of data principals/owners with respect to their personal data are protected."*

3.8.6 Clearly mention 'lawfulness', transparency and fairness as a standard. Personal data shall be processed fairly and lawfully which means that information should be processed on a clear legal basis, for a lawful purpose, and in a fair and transparent manner so that users are adequately informed about how their data will be collected, used, or stored, and by whom.

3.8.7 Specifically mention ‘data minimisation’ as one of the standards - *“Personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose”*

3.8.8 With respect to Clause 26.2 of the Policy, which states that in the interest of transparency, data fiduciary must “make certain information available”, we suggest:

(a) The Policy must clearly state to whom the ‘information to be available’ and in what form. Will it be put up on a board in a facility? Will it be given out as IEC material or become part of the privacy notice for informed consent?
(b) Clause 26.2 (c) Policy must clarify what exactly is meant by “personal data processed in exceptional situations" and “any exceptional purposes of processing”, so that the ambit of these ‘exceptions’ are precise and clear; and there is clarity on whether such processing will be done without consent.
(c) Clause 26.2(d) The data fiduciary must ‘list down’ the rights of the data principals/owners; procedure of exercising these rights; and availability of grievance redress mechanism for complaints regarding data breach.
(d) Add breach notifications, “the data fiduciary will inform the data principal/owner as soon as any breach occurs and take steps to contain it, and also advise data principal/owner to take steps to minimize any harm that may result from such breach. Further, a record of any breach and steps taken thereon, must be recorded and maintained.”
(e) The Policy must specify what is meant by “important operations” in the processing of personal data and if it includes operations for which a specific consent was not given. Also, this should be independent of and without prejudice to the right of the data principal/owner to exercise their ‘right to information’.

3.8.9 Move clauses on Purpose limitation (26.5), storage limitation (26.6), accuracy/data quality (26.8) to before the clause on privacy by design. This is because privacy by design and default essentially means compliance with all the standards.

3.8.10 Under Clause 26.3 of the Policy on privacy by design, include the following: “The data fiduciary must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, encryption, de-linking, anonymisation, pre-defined role-based authorized access, which are designed to implement data-protection principles, as listed in the Policy in an effective manner and to integrate the necessary safeguards into the processing, in order to protect the rights of data principals/owners.”

3.8.11 After Clause 26.3 of the policy, add a separate clause on “privacy by default” which reads as, “The data fiduciary must implement appropriate technical and organisational measures for ensuring that, by default, only personal data, which are necessary for each specific purpose of the processing, are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the data principal’s intervention to any number of persons or entities.”

3.8.12 Under **Clause 27 of the Policy on** demonstrating adherence to privacy by design and default, add the following:

(a) There should be a **separate section, particularly for producers of technology products, services and applications requiring them to embed privacy and data protection features** and features that support exercise of rights of users, during the designing and developing of such producers, services and applications.

(b) An approved certification mechanism should be used as an element to demonstrate compliance with the requirements of ‘privacy by design and by default’, applicable to both producers of technology and data fiduciaries.

(c) A certification of compliance with ‘privacy by design and default’ should be key consideration in selecting appropriate technology products and platforms for processing of personal data by data fiduciaries. Further, it should become compulsory in public tenders.

3.8.13 Clause 27.2 of the Policy should include guidelines for the terms and conditions within which a data fiduciary may enter into a contract with data processors. State clearly the extent to which data processors will be bound by confidentiality clauses and non-disclosure agreements signed between data principles and data fiduciaries; and what will be done with the data provided to and processed by data processors once the contract between a data fiduciary and data processor ends. The Clause may include a standardized format for contract/agreement with data processors to ensure inclusion of all the necessary clauses.

3.8.14 A clause must be added about contracts between health facilities with producers/vendors of technology products and services, especially EHRs.

(a) Ownership of digital health records in the form of EHRs must be provided by in law, as it will impact several legal rights of the data principals, physicians and technology vendors and have significant bearing on the clauses of contracts between data fiduciaries and technology vendors. While historically there has

been an understanding that patients own the information contained in their medical records, and that providers own the record itself, the current lack of a law governing the ownership of medical records will pose a conundrum when records are stored electronically.

(b) Question of 'ownership' over EHRs also implicates determination of intellectual property rights, mainly the copyrights and patents. Most contentious, however, are the copyrights as they directly relate to issues relevant to medical record ownership, and are often the most ambiguous. Although medical information is not considered intellectual property, the expression of these records in a fixed form may be needed for determination of property rights over EHRs, in addition to medical data, is essential to prevent information blocking and consequently impediments to interoperability.[13]

(c) Upon review of publicly available vendor contracts mainly in the United States of America, two main problems emerged:'limitation of liability' and 'denial of access rights'.[14] In many cases, access to the EHR can be immediately denied to both physicians and data principals, upon nonpayment, allegations of misuse, or in their "sole discretion" if someone with access may jeopardize the confidentiality; may violate the agreement, and/or violate someone's rights. The agreements don't have any clause on how the doctors can access records if needed. A patient's health and life may be seriously jeopardized if access to EHRs is blocked. Further, it would also violate the access rights of the data principal themselves.

(d) In the US, EHR vendors have been known to hit the kill switch and prevent access to patient data in the event of a payment dispute or after the termination of an agreement, even when it has been strictly prohibited by HIPAA.[15]

(e) For these reasons, it is recommended that even in the absence of law, the Policy should also provide some guidance on the necessary elements of a vendor contract outlining the respective rights and responsibilities of a health care provider organization and its EHR vendor, that creates obligations on both parties with respect to the acquisition, implementation, and access and use of an EHR, as well as related transition issues.

---

[13] Jessica Carges (2017), Property Rights and Electronic Health Records. Available at: https://asp.mercatus.org/people/jessica-carges; The Role of Intellectual Property, Law Commission of Ontario. Available at: https://www.lco-cdo.org/en/

[14] Who Owns Patient Medical Records?, The Journal of Urgent Care Medicine (JUCM). Available at: https://www.jucm.com/owns-patient-medical-records/

[15] EHR Vendors Violate HIPAA Rule by Blocking Access to ePHI. Available at: https://www.hipaajournal.com/ehr-vendors-violate-hipaa-rules-by-blocking-access-to-ephi-3611/

3.8.15 With respect to Clauses on ‘data protection impact assessment and ‘audit trails’, it is recommended that absent a data protection law and health sector specific law, these requirements should be tied to accreditation or continued participation in the National Digital Health Ecosystem and related services of telemedicine, e-prescriptions, use of mobile applications etc.

3.9 Protocol for sharing of personal data

3.9.1 Chapter VI of the Policy provides the framework for sharing of personal data with Health Information Users (HIU), sharing of personal and de-identified data for research, obligations of health information users, and restrictions on sharing, circulating and publishing personal data.

3.9.2 At the outset, the framework for sharing of personal data and personal sensitive data of data principals, must ensure transparency and accountability.

3.9.3 The data principal has the right to information which is reasonably required to make informed transactional decisions, especially with regard to revoking consent for sharing data and seeking redress. The data fiduciary must disclose this information to the data principal. Clause 28.3 of the Policy rightly obligates the data fiduciary to maintain a record of consent obtained from the data principal for sharing of personal data. However, the objective of doing so is limited to audit and review. This is not sufficient because the data fiduciary is not required to disclose the information to the data principal, in turn frustrating the right to information. Hence, in addition to maintaining a record of consent obtained, the data fiduciary should be obligated to: (a) maintain a record of the personal data shared with the HIU; and (b) share a record of the consent obtained and personal data shared with the data principal.

3.9.4 Clause 29.1 of the Policy provides an illustrative list of the purposes for which such data may be shared. While it is not feasible to provide a definitive list of purposes, Clause 29.1 should specify that the purposes should be limited to medical and public health research. It is also pertinent that Clause 29.1 should specify a list of purposes for which sharing of anonymised or de-identified data is prohibited and unauthorised. As an example, Section 16 of the Australian Health Records Act, 2012 prohibits sharing of de-identified data with insurance companies.

3.9.5 Clause 29.2 of the Policy lays out the procedure for approval to access anonymised or de-identified data. There are two deficiencies. First, there is no clarity as to who will be providing approval for such access, the data fiduciary or NDHM. Second, the clause does not expressly include the requirement for obtaining the consent of the

data principal prior to sharing, like under Section 15 (ma) of the Australian Health Records Act, 2012.

3.9.6 Under Clause 29.4 of the Policy, the process of anonymisation or de-identification will be formulated at a later stage. In light of this, there is no clarity on the terms and conditions under which data will either be anonymised or de-identified or both, as well as the robustness of these processes to protect and promote the privacy of data principals.

3.9.7 In light of this, we suggest the following modifications to the sharing protocol under Chapter VI of the Policy:

(a) Clause 28.3 should include the obligation to maintain a record of the consent obtained and personal data shared with the HIU, and the obligation to share a record of the consent obtained and personal data shared with the data principal.
(b) Clause 29.1 should limit the purpose of accessing data to medical and public health research.
(c) Clause 29.1 should include a list of purposes for which sharing of anonymised and de-identified data is prohibited and unauthorised.
(d) Clause 29.2 should clarify the authority which will grant approval for accessing anonymised and de-identified data.
(e) Clause 29.2 should expressly include the requirement of obtaining the consent of data principal, in accordance with Chapter III of the Policy, for sharing of anonymised and de-identified data.
(f) The technical processes and anonymisation protocols should be formulated and approved, including the process of public consultations, prior to implementation of the Policy.

3.10 Enforcement

3.10.1 Chapter VII of the Policy provides the framework for enforcing the policy. Clause 32 proposes a process through which data principals may redress grievances with data fiduciaries; Clause 33 obligates the data fiduciary to formulate and implement a personal data breach management mechanism; and Clause 34 empowers the NDHM-DPO as the principal authority for compliance of the Policy; and Clause 35 imposes penalties for any breach.

3.10.2 At the outset, protection and privacy of personal health data is one of the core principles of NDHM and the Policy. This involves a two-pronged approach: prevention and cure. Prevention entails certain rights to data principals to protect their interests.

Cure entails the creation of an independent redress agency where data principals can seek redress. Chapter VII contains deficiencies on both accounts.

3.10.3 Under Clause 32.2, the data principal shall make the first complaint to the internal Grievance Redress Officer of the data fiduciary, while the procedure to redress the complaint is left to the discretion of the data fiduciary. The Clause only specifies the time period within which a complaint should be resolved. This can lead to arbitrary rejection of complaints by the data fiduciary. As an example, one of the most common complaints against Indian health insurance companies, who are free to lay down their own procedure for settlement of insurance claims, is the rejection of claims without any reasoning.[161] In order to avoid a similar problem, the Policy should lay down the procedure for receipt and redress of complaints. This procedure should be embedded in the rule of law.

3.10.4 Under Clause 32.3, if the complaint is not resolved by the internal Grievance Redress Officer, it may be referred to the NDHM-DPO. This is problematic because the NDHM-DPO is already performing executive functions by ensuring implementation of the policy. Like the Blueprint provides a clear separation between the legislative and executive functions of the NDHM, it is also important to ensure separation of judicial functions from other functions. Hence, appeals against orders of the internal Grievance Redress Officer should lie directly with the NDHM. The NDHM should appoint another officer who will be responsible for grievance redress only. This officer should be separate from the NDHM-DPO. As long as the officer discharges adjudicatory functions, he/she should not be involved in other functions. Further, the procedure for settlement of appeal should be provided in the Policy.

3.10.5 Under Clause 32.4, appeals from the NDHM-DPO lie with the Ministry of Health and Family Welfare or through litigation. The rule of law requires that a clear judicial process should be laid out for persons who seek to challenge regulatory actions. There are two deficiencies with the process under Clause 32.4. First, the right of appeal is available to the data principal only, and not the data fiduciary. Second, the proposed appellate structure is vague and outdated. Clause 32.4 creates multiple appellate authorities, including the government and the judicial system. While the rationale for including the Ministry of Health and Family Welfare as one of the appellate authorities is not clear, the other option, “redress through litigation”, is vague. Clause 32.4 should

[16] Malhotra Et Al (2018). "**Fair play in Indian Health Insurance**," Working Papers 18/228, National Institute of Public Finance and Policy (pp. 19-20).

specify a clear appellate structure. It should include a first appeal to the Telecom Disputes Settlement and Appellate Tribunal and a second appeal to the High Court, as specified under Sections 57 and 62 of the Information Technology Act, 2000.

3.10.6 Clause 32.5 obligates the NHA to publicise the procedures for grievance redress and Clause 33.1 obligate data fiduciaries to publicise the personal data breach management mechanism. Awareness about various processes and mechanisms for grievance redress is essential to seek redress. Hence, it is not sufficient that these processes and mechanisms are made publicly available. The data fiduciary should be obligated to disclose this information and also any material change to the information, so that the data principal can make informed decisions, especially regarding the sharing of personal health data. The information should be presented in a legible and reasonably plain language to the data principal.

3.10.7 Under Clause 35.3, the data principal can also seek remedies under other applicable laws. For the sake of clarity and convenience of data principals, the applicable laws should be clearly specified in the Policy.

3.10.8 In light of this, we suggest the following modifications to Chapter VII of the Policy:

(a) The procedure for redressal of complaints should not be left to the discretion of the data fiduciary. Clause 32.2 of the Policy should clearly specify the procedure, in accordance with the rule of law, for receipt and redress of complaints by data fiduciaries.
(b) The NDHM-DPO should not have any role in the adjudication of complaints under Clause 32.3 of the Policy. Appeals against orders of the internal Grievance Redress Officer should lie directly with the NDHM. The NDHM should appoint an officer, separate from the NDHM-DPO, who will perform adjudicatory functions only.
(c) The Ministry of Health and Family Welfare should not function as the appellate authority under Clause 32.4 of the Policy.
(d) Clause 32.4 of the Policy should clearly specify the appellate structure. The appellate structure should include a first appeal to the Telecom Disputes Settlement and Appellate Tribunal and a second appeal to the High Court, as provided under Sections 57 and 62 of the Information Technology Act, 2000.
(e) Under Clauses 32. 5 and 33.1 of the Policy, the data fiduciary should be obligated to disclose information on the process for grievance redress and the personal data breach management mechanism to the data principal. The information should be disclosed in a simple and legible language.

(f) Clause 35.3 of the Policy should specify the applicable laws under which data principals can seek remedies.

Annexure 1

The Policy, read with accompanying guidelines and documents issued under NDHM, contravene and contradict several existing statutory provisions. Government cannot amend or supersede statutory rules by executive action or administrative instructions.[17] Any order, notification, direction or notification issued in exercise of the executive power of the state which is contrary to any other statutory provision, is without jurisdiction and is a nullity.[18] The Policy mentions guiding principles and states that the details of process and procedures and implementation of different aspects, will be laid down by NHA from time to time (It is necessary to point out that NHA is not a statutory authority). So, the policy has to be read together with the guidelines and other instructions issued by NHA. On a reading of the Policy and other guidelines and materials, there emerges at least two areas where the policy/ guidelines/instructions are contrary to existing statutory provisions:

1. Violation of Aadhaar Act and Aadhaar judgement of the Supreme Court in the Puttaswamy Case. While the Policy says that the use of Aadhaar will be voluntary for creating a UHID, the FAQs on NDHM website specify that Aadhaar Card would be mandatory for doctors for creating a digidoctor id. See relevant extract below:

> *"2) Is Aadhaar mandatory to create a DigiDoctor ID?*
> *In Phase I, an Aadhaar enabled DigiDoctor ID is necessary to authenticate the doctor and enable them to e-sign documents. Later versions will allow doctors to enroll using other ID Proofs as well."*

Similarly, the FAQ on Health Facility Registry says,

> *"10) What do I need for registering in the Health ID?*
> *A user needs to register using his Aadhaar and his/her registered mobile number linked to the Aadhaar. Once registered, he/she will be automatically directed to the HFR module."*

[17] Jagit Singh v State of Punjab AIR (1978) 2 SCC 196; Mahadeo Bhau Khilare v. State of Maharashtra SCC (2007) 5 SCC 437
[18] State of Sikkim v Dorjee Tshering Bhutia 1991 AIR 1933

The mandatory use of Aadhaar for creating Digidoctor ID for doctors and Health ID for health facilities is contrary to the Aadhaar Act post the judgement of the Supreme Court in the *Puttaswamy Case*. At the very least, mandatory use of Aadhaar will have to be supported by notification under Section 7 of AADHAAR Act and no such notification have been issued yet. Further, even the voluntary usage of Aadhaar for creating UHID requires a notification under Section 4 of Aadhaar Act. It is not clear if such a notification has been issued.

2. Provision on 'storage of medical data' under the Policy and the accompanying guidelines are contrary to the IMC Act, PCPNDT Act, MTP Act and militate against data protection principles of 'storage limitation' and "right to erasure' and 'right to withdraw consent'. On the contrary, Clause 14.1(b) of the Policy includes the 'right to erasure', but provides that if storage for a certain period is mandated by law then the data cannot be erased. It would follow that erasure can be requested as a right when the statutory period is over. But Policy says that "personal data can be blocked and restricted rather than erased" and that "if erasure is not possible without disproportionate effort due to the specific type of storage, over-writing, other means of removal can be used." The language does not guarantee the right of erasure and data can be stored even after the statutory period is over on flimsy grounds. However, the NDHM Strategy Overview document states that "Health Information Providers (HIPs) will keep a digital copy of both inpatient and outpatient health records they issue to patients as per policy. The current guidelines issued by MoHFW requires care providers to store medical records digitally indefinitely" (Federated architecture of health data at 2.2.4 (2)). The refusal to erase medical data once the statutory period is over and any Instructions to store medical records indefinitely is contrary to existing statutory provisions, and even goes against express statutory provision to delete such data, for instance in the Medical Termination of Pregnancy Act (See below). to out that the people should have an absolute right to get their medical records deleted after the statutory period of storage is completed:

    a. Under Indian Medical Council Act, Regulation 1.3.1 of the Code of Ethics Regulation 2002 requires physicians to maintain the medical records of their patients for a period of three years only.
    b. Under the Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (PCPNDT), all records of pregnant women who have undergone an ultra sonography must be preserved for a period of two years. The Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Rules, 1996 (PNDT

Rules) require that when the records are maintained on a computer, the person responsible for such record should preserve a printed copy of the record after authentication.

c. Under the Medical Termination of Pregnancy Act 1971, hospitals have to maintain an Admission Register of women who have terminated their pregnancy. Under Regulation5 of the Medical Termination of Pregnancy Regulations 2003, the record must be destroyed on the expiry of a period of five years from the date of the last entry. The Act stresses the importance of secrecy and security of information. Hospitals are prohibited from disclosing the information contained to anyone. The admission register is considered ‘secret’ and stored in safe custody of the head of the hospital.