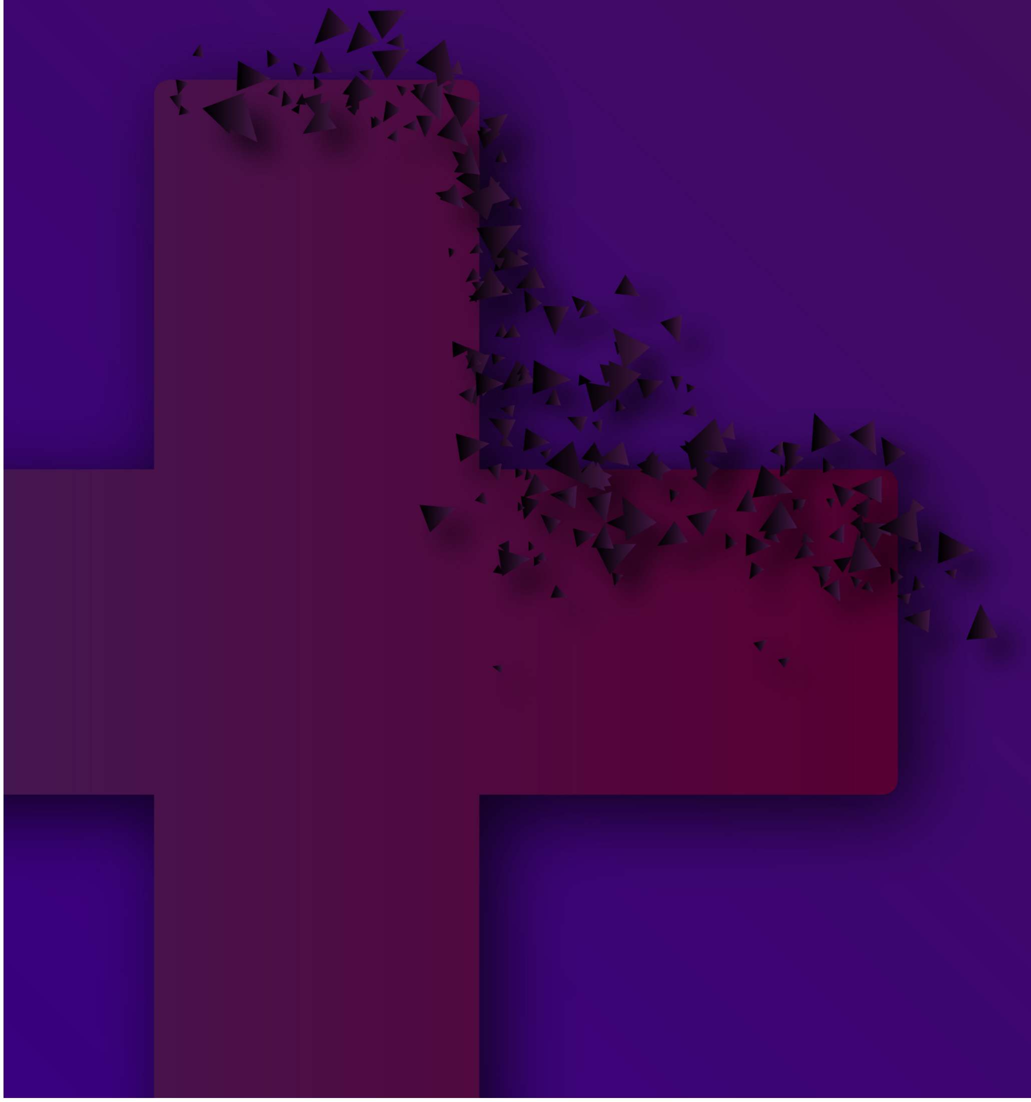
The Dialogue™
INFORM ENGAGE IDEATE

RESPONSE TO DRAFT HEALTH DATA MANAGEMENT POLICY



National Digital Health Mission: Health Data Management Policy

Authored by: The Dialogue, New Delhi
Editor: Kazim Rizvi[1]
Cover Illustration: Abhinav Kashyap

[1] Founding Director, The Dialogue

Table of contents

List of Abbreviations

1.	DISHA	Digital Information Security in Healthcare Act
2.	EU GDPR	European Union General Data Protection Regulation
3.	HIP	Health Information Providers
4.	HIU	Health Information Users
5.	NDHB	National Digital Health Blueprint
6.	NDHE	National Digital Health Ecosystem
7.	NDHM	National Digital Health Mission
8.	NPD	Non-Personal Data
9.	PDP	Personal Data Protection Bill
10.	SPD	Sensitive Personal Data
11.	DPO	Data Protection Officer
12.	MoHFW	Ministry of Health and Family Welfare
13.	MeitY	Ministry of Electronics and Information Technology

1. Executive Summary

At the outset, we would like to thank the Ministry of Health and Family Welfare for inviting comments on the National Digital Health Mission: Health Data Management Policy", which forms a part of the larger National Digital Health Mission (2017) from the public and ensuring the participation of civil society in the lawmaking process.

The Dialogue hopes to aid the Government in conceiving a comprehensive framework for the management of the health data while balancing both the objectives of the State and a citizen s right to privacy as envisioned by the Supreme Court of India in the K.S Puttaswamy vs. Union of India judgement.

As a part of our submission we have commented on particular aspects of the policy that can be built upon further and have also tendered our recommendations on the same. Please find below a summary of our comments and recommendations, followed by a detailed account of the same.

Definitional clauses
This section speaks about the definitional clauses enlisted in this policy. As the policy is expected to operate under the larger umbrella of protection being provided by the Personal Data Protection Bill, this section seeks to highlight the issue of ensuring harmony between legislations and ensuring that they are drafted in the vein of complementing one another. The section highlights the need for defining health data to provide an added layer of protection to ordinary data that may be at the risk of giving away sensitive health related information of an individual upon processing or combination with other personal data. There are certain definitions which need to be defined in order to remove vagueness, like Health Information exchanges, digital health records etc. It also needs to be considered that if health is a state subject, why was there no involvement of states while building the particular policy.

Consent Architecture
The section talks about the consent architecture as laid down by the said policy. The whole policy is touted to be voluntary in nature based on the consent of the data principal. However, the policy lacks an understanding of the Indian sociological context in terms of its literacy and understanding of the privacy policies and informed consent. Thus, the section talks about different models of consent which India can adopt and the issues surrounding interoperability.

Creation of Health ID

This section discusses issues pertaining to the issuing of the Health ID. We primarily examine the manner in which data will be compiled and stored, and the resulting compromise on citizen privacy and security. We explore the Aadhaar based verification mechanism and highlight the challenges associated with mandatory linking. Furthermore, we discuss the voluntary nature of registering for the aforementioned health ID and underline the importance of why it should never act as an excluding factor.

Sharing models for anonymization

The section assesses the sharing mechanisms of anonymized personal data among important stakeholders. A tool which is at the heart of security as it prevents de-identification of data thus ensuring privacy needs to be examined in detail. We suggest certain anonymization techniques which the government can study and can frame a technical expert committee for the periodic audit of these techniques deployed in the healthcare sector. Thus, this section provides the blend of both theory as well as technical concepts needed to strengthen security.

National Digital Health Mission - Data Protection Officer

This section discusses the role of the National Digital Health Mission-Data Protection Officer. The purpose of the officer is to ensure legal compliance to the NDHM, communicate with regulators and external stakeholders on data privacy, review security safeguards periodically and redress complaints not adequately handled by the data fiduciary. This submission raises questions on how many DPOs would be needed by a state, the transparency in hiring a government officer as a DPO, accountability mechanisms, the role of the DPO with respect to the proposed Data Protection Authority and Non-Personal Data Protection Authority in the future of India s data protection regime and inclusivity and diversity in hiring the DPO.

Grievance Redressal Mechanism

It also covers the process of Grievance Redressal as elucidated by the said policy. The Section highlights how the policy fails to acknowledge the pre-existing mechanism under the PDP framework and bypasses the said mechanism by creating its own authority and also does not allow for the appeal framework to include the pre-existing systems as per the PDP.

Comparative analysis of health data management frameworks of the US and European Union

Section 8 provides us with a more comprehensive understanding of the workings of health data management frameworks through a qualitative analysis of best practices. For this, we examine health data policies in the United States and the European Union, considering their relatively developed digital ecosystems and data protection frameworks. This gives us an appreciation of the more progressive policies put in place while steering away from the pitfalls that these countries encountered.

2. Definitional Clauses

The National Health Digital Mission largely employs the use of the definitions that have been used through the Personal Data Protection Bill, 2019[2] (PDP Bill). Important definitions relating to data and processing such as those of processing, data principal, data fiduciary, child, data, data processor, de-identification remain the same as those under the PDP Bill. However, the policy has added certain specific definitions and expanded the scope of certain terms to include an added layer of protection to health-related data.

Expansion of Sensitive Personal Data - Clause 4(ee)

The policy expands the definition of sensitive personal data (SPD) (4(ee)), as compared to that found in the PDP Bill, to include physical, physiological and mental health data”. The expanded definition also includes within its scope information pertaining to an individual s health conditions and treatments, which includes their Electronic Health Record (EHR), Electronic Medical Record (EMR), and Personal Health Record (PHR). The definition also provides an expanded explanation to financial data, a feature that is absent in the PDP Bill, 2019.

It is pertinent to note that PDP Bill, 2019 already enlists health data as a category of sensitive personal data as per Section 3(36), PDP Bill 2019. The said policy however once again expands the scope of sensitive personal data by providing explanations and expansions to its pertaining to health related data of an individual, however it fails to define and elucidate the meaning of health data” succinctly.

As this policy is specifically aimed at the management of health data and the definition for SPD as per the proposed PDP Bill already includes a category termed health data , we recommend that this policy is utilised as an opportunity to define of the term health data or explain what the category of health data under Sensitive Personal Data as per the PDP entails to cover. We believe that this would help reduce complications that may arise from having varying definitions for standard terms such as sensitive personal data across different legislations.

As health data is already an indicated subset of sensitive personal data, a definition specifically pertaining to health data would help provide an added layer of protection

[2] Personal Data Protection Bill, 2019, MInistry of Electronics and Information Technology, Government of India, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

that covers scenarios where ordinary data in combination with other data may lead to sensitive health related data being shared for commercial or state interests beyond the permitted limit of processing for which an individual has provided explicit consent.

Such an approach of defining health data is not unprecedented in data governance frameworks, as the EU GDPR also employs a definition for health data. Article 4(15) of the EU General Data Protection Regulation (GDPR), defines data concerning health as: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”

A similar approach is also taken by the law in France, though the French Data Protection Law does not explicitly define health data, the CNIL (French Data Protection Authority) through its mandate considers any information which is capable of identifying the nature of an illness, a handicap or a deficiency should be considered as health data”.[3]

Ideally, this policy is expected to operate under the larger umbrella of protection that is to be provided to data via the Personal Data Protection Bill, 2019. Hence, it must best complement or enhance nuance in matters relating to health data as opposed to having contradicting or varying definitions. It is imperative that such frameworks that are targeted at specific sectors endeavour to have interoperability with the PDP framework rather than creating entirely independent frameworks and mechanisms.

As the said policy itself mentions the notion of creating systems that are privacy respecting”, the aim of the legislation must be to provide protection to a person's data related to or with the potential to indicate or divulge sensitive health related data of individuals. (In some circumstances on its own or in combination with other personal data).

To serve this purpose and to provide parity among legislations, rather than reinventing or redefining the term sensitive personal data”, we propose to clearly define a criterion for health data” that would ensure better protection to an individual s data and also reduce implementational uncertainties by harmonizing the said policy with the proposed data frameworks for NPD and PD.

[3] https://www.cnil.fr/sites/default/files/typo/document/FICHE7_PackConf_LOGEMENT_SOCIAL_web.pdf

Multiple undefined terms

Certain key terms remain undefined throughout the entirety of this policy that may create hurdles during the process of implementation of the said policy.

Digital Health record

For e.g. Digital Health record . Although the policy begins with the stated purpose that the Government of India intends to digitise the entire healthcare ecosystem of India through the creation of digital health records, it fails to provide clarity of whether these digital health records are to be treated at parity with the electronic health records. A clearer definition or guidance through the policy would be a welcome move in this regard.

Point of care

The term Point of care is used in Clause 26.3 (which deals with Privacy by design for frameworks developed under this policy) for the first time across any legislation pertaining to data protection. However, it is important to justify the meaning of the term, through a clear definition, as that is where the personal data of the data principals will be stored. It is well lauded that the Government intends to frame a federated architecture for storage points but falls short of defining these important points.

Health locker

Clause 4(u) talks about the definition of health locker and states that it would be an information exchange of electronic health records or electronic medical records. It needs to be clarified that the health locker under this policy and Health Information exchange defined under DISHA 2(1) (h) is the same to remove any ambiguities.

Recommendations:

a. Define the term health data to provide clarity on what data entails health data, rather than expanding the scope of sensitive personal data. As sensitive personal data already includes health data as per the PDP, we suggest that the term health data is defined so as to complement the existing framework.

b. Ensure that certain key terms that have been left undefined (Digital Health Record, Point of Care, Health Locker) are defined to provide clarity during the implementation process.

c. Ensure harmonization of definitions across different data governance frameworks rather than having contrasting or contradicting definitions with pre-existing or proposed legislations.

3. Consent Models & Interoperability

For the purpose of allowing for individual control over health data, the Government of India introduced the Digital Information Security in Healthcare Act, 2018 (DISHA”). Combined with the Personal Data Protection Bill, 2019 (PDP Bill”), the health data of an individual falls within the ambit of both these legislations. . While the PDP Bill deals with all kinds of health data, DISHA is limited to digital health information only. With the boom in the healthcare sector in India, it is likely that a substantial chunk of health data will be moving into a digital format, thus warranting more scrutiny in the laws that apply.

Under DISHA, the user has been given the power to control the flow of his/her data at every stage of data collection, processing, storage, transmission, etc. Moreover, the user has been given the power to refuse the consent for data collection at any stage he/she wants. The consent mechanism under the PDP differs in this regard. Under the PDP bill, health data is classified under the sensitive” category. This in turn mandates the explicit consent to be sought before data collection for the specified purpose, only at one stage. DISHA imposes that at every stage of collection and transmission of data, explicit consent needs to be sought. This creates two separate standards for the governance on the same subject matter.

This difference in standards of collection of consent for the purpose of data sharing, data collection and processing creates uncertainty for compliance and weakens user protection. Having widely differing standards also leads to regulatory arbitrage where the businesses can pick and choose the less burdensome regulation to suit their needs.

Clause 3(c) states the objective of this policy and one of them is to a system which is voluntary in nature, based on the consent of individuals, and in compliance with international standards such as ISO/TS 17975:2015, and other relevant standards related to data interoperability. However, there are issues in relation to both Consent framework as well as interoperability standards, some of which are detailed below.

Consent Framework

Clause 8 (a) stipulates that data principals would be given complete control over the manner in which data is collected and processed and further appropriate technological means would be made to ensure integrity of access permissions.

Designing systems for collecting informed consent for use of data must not lose sight of the social context in which these systems will operate. Considering the lack of digital literacy and long drawn privacy policies that create consent fatigue" amongst its users, implementing a truly effective consent framework might prove to be difficult.

It would be prudent to shift towards graduated consent , in which data principals can give consent to anonymization for each type of data throughout their contract with the service provider, rather than just having a binary choice. A model of consent collection that limits the period for which a consent will remain active for, is worth exploring. This would be complementary to the four principles stated above.4

For example, there are electronic marketing calls or bank calls etc. which generally do not ask for the caller s permission to record the call, and makes its mandatory on the user to be recorded for security and training purposes" Even though there has been changes in operations of some companies that follow this, there's a lot of work to be done before it can be cemented as an industry practice. In case of such calls/methods of data collection, where consent can be taken for a particular time frame, could be useful to add nuance to the existing requirements. In the example stated above, that would mean that the recipient of the call has previously notified the caller that he consents for the time being to such communications being sent by, or at the instigation of, the caller".

Helen Nissenbaum in her Theory of Contextual Integrity has indicated how long consent can be generally relied on, and most often it is based on the context. The phrase time being" is of importance here. Granted that a user might consent to the use of data to anonymize or aggregate datasets as the privacy policies indicate. However, on the launch of new features in that same product, it cannot be a case of ongoing consent. This is where graduated consent plays its role.

Further, the report does not talk about maintaining records of consent which records the date of consent, what information was provided to the person consenting etc. These records of consent are necessary as a proof to compliance and auditing purposes.

[4] Royal Academy of Engineering, "*Connecting data: driving productivity and innovation. Royal Academy of Engineering*", 16 November 2015. Available at http://www.raeng.org.uk/publications/reports/connecting-data-driving-productivity.

Recommendations:

a) Different consent models should be designed and deployed, for e.g. Graduated consent.

b) Apart from the four principles of consent in the PDP Bill, a fifth principle of time being consent should be thought about and implemented accordingly.

Interoperability

One of the core objectives of this policy is a consent framework that has already been discussed, but it is to ensure interoperability across all players of the NDHE. The policy is lauded in terms of accepting that there are multiple applications, programming languages, and platforms in India through which interoperability can be functioned, however, India lacks a national standard or sector-specific standards on interoperability. There are two barriers that need to be addressed in this regard.

Firstly, we must aim to enhance the capacity of workers in the healthcare sector who deal with the process of data entry. It has been noted that data entry operators are working under immense burden and workload5.

Secondly, due to consolidation and privatisation of HIPs countrywide, it gives rise to centralised databases. Thus, there is a need for federated architecture in order to obviate cybersecurity risks and value the consent of the data principal.

Recommendations:

a) Focus should be on capacity building, resource allocation and training of data entry operators as data would not be always digitized.

b) In order to come up with a federated architecture, different categories of data would be stored in different silos. This would also be in tandem with NDHB which requires bulk of the information to be managed in a distributed model, however should be more specific with the meaning of bulk.

[5] BHATTACHARYA, M., SHAHRAWAT, R., & Vinod, J. O. O. N. (2012). Understanding level of maternal and child health indicators used in Health Management Information System among peripheral level health functionaries in two districts of India. *Journal of Health Informatics in Developing Countries*, *6*(1).

4.Creation of a Health ID

The Health Data Management Policy Draft proposes the creation of a health ID to centralise data storage and expedite access to patient data across medical institutions and platforms. The ID allows individuals to participate in the NDHE and we appreciate the intention here. Having said that, there are aspects of the introduction of such an ID that could be challenging.

The questionable nature of the voluntary” feature of registering for the health ID has been brought into the spotlight with reports emerging of doctors working in government hospitals of Chandigarh being compelled to register for the ID despite it not being mandated6. Section 15.27 of the policy discusses the use of the Aadhaar card for verification purposes to aid the creation of this health ID.

While the draft does mention that linkage is not mandatory in Section 16.3, the counterfactual is not discussed and there exists precedent for cases where such decisions have been rolled back.
The Supreme Court in 2018 had stated that linking benefit schemes with Aadhaar shall not be made mandatory.

Lack of an Aadhaar ID could exclude individuals from obtaining a health ID and impeding their overall access to healthcare services. While the very origin of centralised ID s such as the health ID and Aadhaar is to reduce leakages and improve access for the poor, the system is a work in progress and we need to tighten the gaps that exist currently.

Recommendations:

a) Move away from centralised data storage systems towards a more decentralised model. This will increase citizen privacy and the overall security of the compiled health data.

[6] Rana, C. (2020, September 10). Chandigarh doctors compelled to register in NDHM registries. Retrieved from https://caravanmagazine.in/health/doctors-in-chandigarh-compelled-to-register-for-the-voluntary-national-health-id

[7] G. (2020, August 27). Health Data Management Policy Draft. https://www.medianama.com/wp-content/uploads/National-Digital-Health-Mission-Health-Data-Management-Policy.pdf

b) Ensure that the voluntary” nature of registration for the health ID is actually translated to reality, and come down on local governments and medical facilities which mandate the same.

c) Launch and scale up the Health ID program only once India s data protection and privacy laws have been passed in Parliament.

5. Sharing of anonymized data by fiduciaries

Data sharing when it comes to anonymised data by fiduciaries would operate under the ambit of the proposed Non-Personal Data Governance Framework and the DISHA Act. The proposed policy permits data fiduciaries to share de-identified or anonymized data in an aggregated form for the purpose of facilitating health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions and such other purposes as may be specified by the National Health Authority. It is important to harmonise and fine tune the purposes for which such data would be shared. The proposed NPD framework also speaks of sharing of health data for similar objectives. Any sharing of anonymised data must adhere to strict standards of security. It must also be restricted to the purpose of sharing specified strictly, and to the extent necessary.

Clause 29 of the said policy talks about sharing of anonymized data specifically about the process of sharing the data in an anonymized form. Clause 29.4 also stipulates the mechanism of choosing anonymity protocols which NHA would do in consultation with MeitY. It also mentions periodic review of such protocols with regards to the nature and sensitivity of the data.

Privacy by design is synonymous to anonymized or pseudonymised data so that it is no longer possible to identify an individual from the data itself or from that data in combination with other data. Though, the NHA will come up with certain techniques stipulated in consultation with MeitY, but it is highly likely that the Primer on Anonymization made by Committee of Experts under Non-Personal Data Draft shall be followed. It is understandable from the fact that there should be a national standard pool of anonymization techniques, among which different sectors can choose to adopt for sharing and storage practices.

We strive to recommend some of the duties HIU can adhere to and also balance between utility & privacy:

Recommendations:

a) HIUs & HIPs needs to be able to show the means of assessing the risk of re-identification, and the proportionate solution adopted by them. While assessing risk, the HIU & HIP shall maintain a balance between the utility of the dataset and the privacy of the citizens.

b) There should be an expert body under MeitY providing advice on anonymization techniques from time to time to keep in line with the best practices globally. Simple consultation of NHA with MeitY under 29.5 is vague in terms of who would be incharge of the periodic review. NHA can refer to the UK Anonymization Network (UKAN)[8] which is a consortium of University of Manchester and Southampton, the Open Data Institute and the ONS.

c) To maintain utility as well as privacy, NHA can refer to the work of J. Domingo Ferre and V. Torra,[9] which examine three procedures to measure the impact of anonymisation: Direct comparison of the categorical data, to obtain average distance between them, Computation of contingency tables of both original and anonymized datasets and the distance between the two, and finally, probabilistic measure which measure the uncertainty on the values of the original dataset given the values of the anonymized dataset.

d) The report does not categorize anonymized data, however, the manner of anonymization would differ between static, dynamic and streaming data. Dynamic data is the case when a database changes with respect to time and data has to be published regularly. For dynamic datasets, the k-anonymous vector space model developed by Guillermo, Abril and Torra[10] can be used as it enables addition of more data continuously while maintaining the k-anonymity property.

e) In the case of streaming data, primarily the challenge is that data is feeded in portions and in an unstructured sequence. For example, as the authors have described in a report,[11] that during winters people commute less by bike due to snowfall. However by knowing a person comes to work by bike and a set of GPS traces, it may not be possible to identify the person in summer, but possible in winter. Thus, static privacy rules are not the way ahead and the new adaptive privacy preservation techniques are required. So, apart from differential privacy, certain perturbative approaches can be considered.[12]

[8] UK Anonymisation Network website http://ukanon.net/.

[9] J. Domingo-Ferre and V. Torra, "Disclosure control methods and information loss for microdata.," in Confidentiality, Disclosure and Data Access.: North-Holland, 2001, http://vneumann.etse.urv.cat/webCrises/publications/bcpi/cliatpasa01Disclosure.pdf

[10] G. Navarro-Arribas, D. Abril, and V. Torra, "*Dynamic Anonymous Index for Confidential Data*," in 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security, 2013, pp. 362-368.

[11] G. Krempl et al., "*Open challenges for data stream mining research*," ACM SIGKDD Explorations Newsletter - Special issue on big data, vol. 16, no. 1, pp. 1-10, 2014.

[12] F. Li, J. Sun, S. Papadimitriou, G.A. Mihaila, and I. Stanoi, "*Hiding in the Crowd: Privacy Preservation on Evolving Streams through Correlation Tracking*," in IEEE 23rd International Conference on Data Engineering, 2007, 2007, pp. 686-695

6.Data Protection Officer

The National Digital Health Ecosystem (NDHE) envisaged in the Health Data Management Policy mentions that the data collected under the ecosystem will be stored at three levels - i.e. the central, state/Union Territory (UT) level and the health facility level. It mentions the principle of minimality at each level. Data minimality is a principle under the core principles of data protection, and essentially places restrictions on the amount of personal data to be collected, and places limitations on what data is necessarily collected.13

Explained under Chapter II: Applicable Law and Governance Structure in the draft policy, this storage is then governed by a structure specified by the National Health Authority (NHA). The chapter specifies that the governance structure will have committees, authorities and officers at the national, state and health facility levels" to implement the NDHM. Moreover, there will be a data protection officer (called the NDHM-DPO) - who shall be a government officer.

FUNCTIONS OF THE NDHM-DPO

The Dialogue has collated the functions of the NDHM-DPO from across the pages of the Health Data Management Policy. The NDHM-DPO will –

1. Ensure adherence to this Policy and shall be responsible for compliance with all applicable laws in force in India (clause 34.1)

2. Communicate with regulators and external stakeholders on matters concerning data privacy and serve as an escalation point for decision-making on data governance and other matters concerning data (clause 6)

3. In the case of any entities who are implementing/involved in the NDHM and acting as a data fiduciary in this regard, the NDHM-CISO and the NDHM-DPO will undertake a periodic review of the security safeguards and take appropriate measures to update such safeguards, if required (clause 27.1)

[13] Privacy Law and Policy Reporter. (n.d.). Retrieved September 20, 2020, from http://www5.austlii.edu.au/au/journals/PrivLawPRpr/2001/9.html

4. In the event that a complaint is not resolved by the Grievance Officer of the data fiduciary as referred to under clause 32.2 above, the matter may be referred to the NDHM-DPO in writing or through an email ID provided under the grievance portal of NDHM website (clause 32.3).

7. Grievance Redressal and Compliance

The policy mentions that if a complaint is not resolved through consultation with NDHM-DPO as referred to in paragraph 32.3 above (or through any other mechanism under existing agreements, if any, between parties such as mediation or arbitration), then the data principal may, at her/his option, seek redressal by way of a complaint to MoHFW or litigation.

Chapter VII of the policy discusses Grievance Redressal and Compliance, and mentions that a data protection officer appointed by the data fiduciary can be approached by data principals - in order to resolve their questions about the processing of their personal data.

This DPO appointed by the data fiduciary will be called a designated officer, or can also be called a Grievance Officer (clause 32.2). The DPO s details will be mentioned on the website of the data fiduciary, and in case the Grievance Officer is not able to resolve a data fiduciary s complaint, then the complaint will be referred to the NDHM DPO in writing or over an e-mail, in a specified format.

Challenges

Appointment of the Government Officer as NDHM DPO
There are certain concerns with respect to the wording of the policy. Firstly, appointing a government officer as an NDHM-DPO raises some concerns - around transparency and independence, especially. The same concerns are raised in terms of the PDP 2019, with government interference in the appointment process. Furthermore, it is not specified whether the NDHM-DPO will be a medical expert or not, or a technical officer. Whether the Ministry of Health and Family Welfare (MoHFW) will have more say in appointing the officer, or the Ministry of Electronics and Information Technology (MeitY), is not specified in the policy.

Overlap with other data governance frameworks
Secondly, the role of the proposed NDHM-DPO seems to overlap with that of the Data Protection Authority under the proposed PDP 2019 and the NPD Authority envisaged in the draft report on regulating Non-Personal Data.14 This regulatory clash is unclear in

[14] Aryan, A. (2020, July 26). Explained: What is non-personal data? Retrieved September 20, 2020, from https://indianexpress.com/article/explained/non-personal-data-explained-6506613/

the proposed documents. By eliminating redressal mechanisms through the Data Protection Authority and the Non Personal Data Authority after a complaint has not been adequately addressed by the NDH DPO fails to utilize pre-existing redressal mechanisms that have been specifically for the purpose of complaints pertaining to data.

Lack of clarity pertaining to adequacy of one NDHM DPO for each State Thirdly, one NDHM-DPO for the entire state does not seem to be adequate. There needs to be an adequate number of NDHM-DPOs, preferably individuals who come from different backgrounds in public health - including women and trans people, who can help data principals ensure their data rights - regardless of socioeconomic barriers such as class, caste, gender, education and so forth.

Accessibility
Fourthly, the policy must address any issues pertaining accessibility to the grievance redressal for a larger section of society and any mechanism/programmes to promote awareness.

The redressal mechanism is limited to a very narrow approach of registering through a designated letter format or via email. Considering India s demographic a large number of data principals may be able to use this mechanism effectively owing to its dependence on conventional and digital literacy. Any grievance redressal mechanism in India must strive to be less text based, more graphic and available in as many regional languages.

Pertaining to awareness, considering the nascent stage of data protection frameworks, every framework must strive to promote awareness of rights and resources under any framework. The provision of instructional videos, step-by-guides to utilise web portals, workshops by the office of the DPO to ensure that various entities at different levels are aware of their responsibilities and obligations.

Recommendations:

a) The NDHM-DPO should be appointed by following a transparent and adequate process - given that health data is one of the kinds of sensitive personal data with scope for immense misuse.

b) The NDHM-DPO should be appointed as an expert from a field of public health. Ideally the office of the NDHM-DPO should have members from data science fields, as well as public health and social science experts working in the health space. There should be an emphasis on inclusivity in appointment, so that the health data rights of different sets of individuals can be ensured.

c) The role of the NDHM-DPO should be seen in tandem with the Non-Personal Data authority (which is proposed in the recent report) and the Data Protection Authority under the PDP 2019. Their roles must have synergy - even on paper and especially in practice. The jurisdiction and scope of each authority s powers must be clear before the implementation of the law.

d) Different states will have different requirements in terms of the number of NDHM-DPOs required. The minimum requirement of the number of officers should be determined after conducting detailed studies about the state of health data practices in a particular state - given that they vary drastically based on state capacity.

e) Any grievance redressal mechanism should strive to have far reaching accessibility, thus we propose a less text based (overall less dependant on literacy) and more graphic mechanism. At present, merely restricting complaints to emails and letters excludes a large population. We recommend easier, more people friendly options such as forms to help individuals file their complaints without professional legal assistance.

8. Comparative Analysis

Creating a comprehensive health data management policy is a complicated task and an important step in the process is examining best practices from different countries around the world. While data governance is an evolving field, there are certain countries which have been working on developing frameworks for a longer time than India and there are lessons we can imbibe from their success and failure. For the purpose of this report we will analyse the policies put in place for health data management in the European Union and the United States.

United States

The United States has a relatively evolved health management system and utilises the data they collect for a multitude of purposes. These include insurance and welfare purposes, tracking patients with specific diagnosis or conditions and drug efficacy data. Considering the sensitive nature of identifiable health data, the American government attempts to implement stringent data collection and access controls, puts in place security measures and even applies reasonable use limitations as well as de-identification practices.

The process of sharing of non-public health data is differentiated based on identifiable and non-identifiable data. Identifiable data poses a larger threat to citizen privacy and we will examine the structures put in place to process this data. In general, identifiable data is restricted in 3 main ways: by internal rules, regulatory requirements and federal legislation. The most broadly applicable is the Privacy Rule adopted under the Health Insurance Portability and Accountability Act (HIPAA), which regulates the use and disclosure of individually identifiable information by covered entities15.

Apart from the legislative actions of the federal government, states also have their own legislation regulating the collection, use and disclosure of health information. For example, nearly every state has some statutory or regulatory provisions that grant individuals the right to access their medical records maintained by medical doctors and/or hospitals."16 Many states have separate laws for specific categories of

[15] Secretary, H., & (OCR), O. (2013, July 26). Summary of the HIPAA Privacy Rule. Retrieved September, 2020, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary

[16] Joy Pritts et al., Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Medical Record Access Laws (Aug. 2009), http://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf

sensitive information such as mental health, substance abuse and disease diagnosis. However, HIPAA supersedes state laws that are less privacy-protective, while allowing states to impose relatively more stringent requirements, hence essentially acting as a baseline requirement for health data privacy within the country.

In addition to the aforementioned regulations pertaining specifically to health data, government agencies are also bound by the Privacy Act of 1974 which regulates the manner in which federal agencies process personally identifiable information. This Act also covers access and correction mandates that give citizens some extent of control over their personal information, including their health data. This extends to the right to know what information was collected, to amend said information, and also some extent of control over the disclosure of this information to third parties17.

It is clear that the American health data protection system is fairly comprehensive and does give citizens some amount of autonomy and rights when it comes to the way in which their data is processed. Having said that, experts agree that having an overarching federal data privacy law makes more sense than the current mix of sector laws and state-level laws. They are attempting to move towards a more decluttered system. Overall, while their system is far from perfect there are multiple important takeaways India can attempt to imbibe while building on our health data management policy.

European Union

Health data and data management are crucial when it comes to empowering citizens and building a healthier society. The European Commission has highlighted its primary goals for health data management within the EU. Some of the primary goals include making health data accessible across the EU through the interoperability of the Electronic Health Record, highlighting the importance of personalised medicine and integrating research data and expertise to improve health prevention and aid diagnosis18.

The EU already has advanced data privacy laws and released new regulations in 2016 relating to data protection and management. The WHO affiliated European Patients Forum then elucidated how these regulations directly impact health data of citizens.

[17] Health Big Data in the Government Context. (2016). *Center for Democracy and Technology*.

[18] Anonymous. (2020, March 08). Managing health data. Retrieved September 2020, from https://ec.europa.eu/digital-single-market/en/managing-health-data

For the sake of our analysis, we will list these features and examine them to gain an overall understanding of their data management framework while also pointing out certain mechanisms that would be helpful tools in the Indian context.

As in the case of the framework that India is attempting to develop, the European Union s health data management prioritises fairness and transparency, with consent expected to be explicit and unambiguous. Data also must be collected for a particular purpose and time period, and should be information that is specific and pertinent to the case of the patient at hand. The EU also places responsibility on the data fiduciary for ensuring there is no misrepresentation or inaccuracy within patient s health data. Furthermore, confidentiality is prioritised and health data which is used for research is processed in the form of unidentifiable anonymised data[19].

India has also developed clauses within our health data management framework which broadly have similar objectives. Considering the universal praise that the EU receives for upholding data privacy, this is an encouraging sign. However, there are two major differentiating factors. Firstly, the European Union has a well-developed data protection framework in the form of GDPR, which acts as a foundation for any subsequent privacy acts. This has resulted in better protection for citizens and has increased effectiveness and implementation of regulations. Secondly, the European Union has created a system of accountability on the part of the data fiduciary. In their framework these data fiduciaries are not only expected to adhere to the principles of the legislation put in place, but also prove that they are accountable and respect the above principles. Essentially, the burden of proof is on these data controllers and this is a productive move that could meet with positive results in the Indian context as well.

[19] The new EU Regulation on the protection of personal data ... (2017). Retrieved September, 2020, from http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf