CUTS International

CUTS Submission of Comments on Health Data Management Policy to The Ministry of Health and Family Welfare

Consumer Unity & Trust Society (CUTS)[1] expresses its gratitude to The Ministry of Health and Family Welfare (MoHFW), for inviting comments and suggestions on the draft Health Data Management Policy.

About CUTS

In its 35 years of existence, CUTS has come a long way from being a grassroots consumer-centric organisation based in Jaipur to opening overseas Resource Centres in Vietnam, Africa, Switzerland, and most recently in the United States of America. It continues to remain an independent, non-partisan and non-profit economic policy research and advocacy group, while working on various programme areas, such as Trade, Economics & Environment; Consumer Action, Research & Training; Human Development; and Competition, Investment & Economic Regulation. It has been working towards enhancing the regulatory environment through evidence-backed policy and governance-related interventions across various sectors and national boundaries. For further details regarding CUTS, please visit: http://cutsinternational.org/pdf/About-CUTS-2018.pdf

Being a consumer-centric organisation, CUTS has observed a few critical issues in the policy, which may impede consumer welfare, either directly or indirectly as a result of suboptimal clauses. Notably, many of these issues are overlapping with aspects of the Personal Data Protection Bill 2019 (the bill or PDPB). The suggestions given below are informed by:

- CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019[2]
- CUTS Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework[3]
- CUTS study 'Data Privacy and User Welfare in India' (Privacy Survey) wherein perspectives of 2160 users of digital technologies with respect to data sharing, purposes thereof and risks therein were considered.[4]

Analysis

The draft policy falls short on account of various aspects. Specifically, the policy deep dives into issues surrounding data protection. However, cross-sectoral principles of protecting personal and non-personal data (like consent, purpose limitation, rights of data principals, obligations of data fiduciaries etc.) are currently being deliberated upon through the Personal Data Protection Bill, 2019 and the draft Recommendations of the Committee of Experts on Non-Personal Data Governance. CUTS comments on such issues being covered under this policy have been given in the table below.

[1] https://cuts-international.org/

[2] https://cuts-ccier.org/pdf/submission-pdpb-2019.pdf

[3] https://cuts-ccier.org/pdf/comments-on-the-report-by-the-committee-of-experts-npd.pdf

[4] Objective: Engage with consumers on a pan India level regarding data and privacy protection on both, online, as well as offline platforms, from the government and private players alike. Expected Outcome: Policy reforms empowering consumers for data privacy and protection. https://cuts-ccier.org/cdpp/

Clause	Issue	CUTS Remarks
Definitions		
4(f)	“consent manager” means an entity or an individual, as the case may be, that interacts with the data principal and obtains consent from him/her for any intended access to personal or sensitive personal data, where the role of the consent manager may be provided by the NHA or any other service provider;	The bill had classified consent managers as data fiduciaries,[5] thereby imposing various obligations on them, such as: purpose limitation, providing notice and taking consent of data principals, providing grievance redress, restrictions on retention of personal data, ensuring quality of personal data etc. Also, the bill required consent managers to provide an accessible, transparent and interoperable platform to data principals for gaining, withdrawing and reviewing their consent. Such provisions make consent managers accountable to data principals (consumers), and are therefore in the interest of upholding consumer welfare. Accordingly, these should be mentioned in the definition of consent managers, as given in the policy. Furthermore, as mentioned in the bill, consent managers are required to be registered with the proposed Data Protection Authority (DPA).[6] It remains to be checked whether consent managers defined under this policy would also require to be registered with the DPA, as well as the National Heath Authority (NHA), and if so, would it lead to duplication of compliance costs. Notably, consent managers are somewhat similar to the Account Aggregator (AA) mechanism which provides a centralised framework for providing consensual sharing of information with financial service providers through Data Protection and Empowerment Architecture (DEPA). Such mechanisms are new for consumers, and there are concerns regarding the acceptability of such

[5] S.23(5) Explanation: a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

[6] S.23(5): The consent manager, shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Clause	Issue	CUTS Remarks
		infrastructure and familiarity of its functioning by consumers, and their adherence to privacy by design policies as proposed under the National Digital Health Mission. Furthermore, there is a need to weigh the security risks posed by having a centralised consent dashboard. Given that consent managers are likely to the act as intermediaries between consumers and service providers, there is a need to avoid conflict of interest and ensure that right incentives are in place to enable them to act in the interests of consumers. For further details, please refer CUTS policy brief on 'Notice and Consent Mechanism', available here.
4(o)	"harm" means, -- (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal;	'Harm' as prescribed in the policy lists certain outcomes which may cause adverse effect on consumers, but does not make a clear linkage to misuse of data. Further, the scope of the definition is limited as it does not take into account new risks which might have to be addressed with evolution of technology. This creates ambiguity and confusion for users and service providers, and limits the rights of consumers to only listed harms. To address this, the policy must provide a broader definition of harm. Also, appropriate guidelines regarding its interpretation to establish linkage between harm and personal data or sensitive personal data of their use must be laid down. The proposed definition also uses terms like 'evaluative decision' and 'reasonable expectation' which are subject to interpretation on a case by case basis. There is need to provide clarity on these terms and their scope, perhaps through examples. For further details, please refer CUTS policy brief on 'Key Definitions under the PDPB', available here.
4(t)	"Health Information Users" or "HIUs" are entities that are permitted to request access to the	The definition in its current form has not defined HIUs adequately. HIUs can be any requesting individual/entity for access to personal data of the data principal,

Clause	Issue	CUTS Remarks
	personal data of a data principal with the appropriate consent of the data principal. The NHA may, from time to time, specify certain terms and conditions in relation to HIUs;	merely based on consent (the effectiveness of which as discussed in subsequent sections is questionable owing to limited awareness and capacity of data principals). More clarity may be provided by the policy in this regard.
4(y)	"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information. For the purpose of this Policy, personal data would include Health ID and Personal Health Identifier;	In its current form, the definition of personal data is contingent upon 'identifiability' of the person through such data. But, this criterion of 'identifiability' may differ depending upon the social, economic, cultural profile and intimacy of the person towards relevant data. This is also informed by the CUTS user perception survey on privacy and data protection, which observed that different consumers (based on gender, age, years of using internet etc.) perceive different information differently. For instance, females are more uncomfortable in sharing their email ids, compared to male counterparts or more adults are uncomfortable in sharing their personal photos compared to younger people.[7] Hence, it is important to consider consumer perspectives while determining 'identifiability' for health-related data, and a consumer perception survey may be conducted in this regard, especially with respect to Health id and Personal Health Identifiers (PHI). Notably, such kinds of data may also fall under the category of Sensitive Personal Data, since the same encompasses physical, physiological and mental health data.[8] Furthermore, as laid under clause 4(z) of the policy, 'PHIs could also be used for re-identifying previously de-identified data. It could include a data principal's demographic and location information, family and relationship information and contact details', thereby making it more

[7] CUTS Study: Users Perspectives on Privacy and Data Protection. Available at: https://cuts-ccier.org/pdf/user-perspectives-on-privacy-and-data-protection.pdf

[8] C.4(ee): "sensitive personal data" means such personal data, which may reveal or be related to, but shall not be limited to, physical, physiological and mental health data.

Clause	Issue	CUTS Remarks
		crucial for consumers.[9] Also, the PDPB also classifies 'health data'[10] as sensitive personal data. Also, the possibility of 'identifying' natural person may differ with relationship of such natural person with the relevant data. Consequently, it might be useful to provide some identifiers and examples to elaborate on concept of 'identifiability' to make it more specific. Such identifiers are also provided within European Union's (EU) General Data Protection Regulation (GDPR).[11]
4(cc)	"pseudonymisation" means a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.	The policy has retained the definition of "de-identification"[12], of the PDPB, but has also introduced a new term, of pseudonymisation. The difference between the two remains blurred, and more clarity may need to be provided on it. Adding to the confusion is 'anonymisation'[13], which also holds a separate meaning. CUTS' recommends such terms to be defined and distinguished clearly in the PDPB, and not in sector specific policies, so as to avoid jurisdictional overlaps and definitional discrepancies between different legislations/policies.
4(ee)	"sensitive personal data" means such personal data, which may reveal or be related to, but shall	No guiding principle is provided at present to distinguish sensitive personal data from personal data and justify greater protection to a subset of personal data.

[9] "Personal Health Identifier" or "PHI" is the data that could potentially identify a specific data principal and can be used to distinguish such data principals from another. PHIs could also be used for re-identifying previously de-identified data. It could include a data principal's demographic and location information, family and relationship information and contact details.

[10] S.3(21): "health data" means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services;

[11] GDPR , Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Available at: https://gdpr-info.eu/art-4-gdpr/

[12] C.4(l): "de-identification" means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to a data principal but does not, on its own, directly identify the data principal;

[13] "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified through any means reasonably likely to be used to identify such data principal.

Clause	Issue	CUTS Remarks
	not be limited to, (i) financial information such as bank account or credit card or debit card or other payment instrument details; (ii) physical, physiological and mental health data; (iii) sex life; (iv) sexual orientation; (v) medical records and history; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; and (xi) religious or political belief or affiliation. For the purpose of this Policy, sensitive personal data would include information relating to various health conditions and treatments of the data principal, such as EMR, EHR and PHR.	The definition also does not take into consideration, consumers perception of privacy, associated risks and perceived sensitivity to different kinds of data. In order to distinguish sensitive personal data from personal data, the specification of associated harms caused due to the revelation of sensitive personal data may be useful. For further details, please refer CUTS policy brief on 'Key Definitions under the PDPB', available here. Furthermore, it remains to be checked whether the examples given under this definition (which have been borrowed from the PDPB), are applicable for the purpose of this policy, such as – caste or tribe; and religious or political belief or affiliation. Such terms may be removed from the policy.
Consent Framework		
8(a)	Data principals should be given complete control and decision-making power over the manner in which personal or sensitive personal data associated with them is collected and processed further.	While the clause is well-intentioned, its practical implementation remains questionable. CUTS study 'Users Perspectives on Privacy and Data Protection', shows that consumers are generally not aware or capacitated to provide consent towards data collection and processing by data fiduciaries. CUTS' recommends the use of innovate digital technologies for devising user-friendly consent mechanisms. Furthermore, model forms for obtaining consent (after notice) may also be provided for in the policy, as laid down under the PDPB.[14]
9, 10 & 11	Consent in relation to collection and processing of personal or sensitive personal data; Privacy Notice for the collection of personal and sensitive personal data; Method of obtaining consent	These issues have been covered under the PDPB, and may not be overlapped in this policy as well, unless for laying any sector specific provisions. For further details, please refer CUTS policy brief on 'Notice and Consent Framework of the PDPB', available here.

[14] S.50(6)(a): code of practice under this Act may include requirements for notice under section 7 including any model forms or guidance relating to notice.

Clause	Issue	CUTS Remarks
	ID Policy	
15.2, 15.7 & 16.3	A Health ID may be authenticated using a data principal's Aadhar number or any other document of identification as may be specified by the NHA. The NHA shall ensure that the means of authentication that are specified under paragraph 15.2 of this Policy do not have the effect of preventing an individual not in possession of an Aadhar number or a mobile number from generating a Health ID.	Given the privacy debate is on-going at the moment, as well as the Supreme Court's judgement, which although upheld the constitutional validity of Aadhaar card, laid down some restrictions on its use and mandatory linkage with bank accounts and telecom service providers; the use of Aadhaar number or similar identification documents may not be the best way of authenticating the Health ID of data principals. Using technology driven modern tools, such as two-step/factor authentication and One Time Passwords, including use of audio and video technology, with appropriate data protection safeguards, may be prescribed in this regard. In any case, technology should only be 'one' of the means for authentication, and need not be the 'only' or 'preferred' means. There needs to be a manual override to ensure that deserved consumers are not deprived of the benefits. The way for such authentication mechanisms is also cleared through clause 15.7 and 16.3, which provide for: 1. Recovery of personal data through means prescribed by the NHA, in case of inability of data principals to access personal data linked with such ID due to any reason; and 2. Non-exclusion of data principals from participating in the NDHE, due to non-availability of Aadhaar number; respectively.
15.3	The personal data of a data principal shall be linked to his/her Health ID, and any data principal in possession of such a Health ID shall be deemed to be the owner of such personal data.	The policy goes a step ahead from the PDPB, and declares data principals as the owners of their personal data linked with their Health ID. Although the same prima facie appears to be a step in the right direction of promoting consumer welfare, however, this issue may have cross-sectoral ramifications, and may set a precedent for other kinds of non-health related personal data as well. Accordingly, this issue may be better deliberated and

Clause	Issue	CUTS Remarks
		addressed under the PDPB, which is currently being debated by the Joint Parliamentary Committee (JPC).
Principle of non-exclusion for Health ID		
16.2	Every data principal shall have the option of opting-out of the NDHE and de-linking their personal data across data fiduciaries, cancelling their Health ID, and requiring the removal of any personal data linked with such ID in accordance with the terms of the Data Retention and Archival Policy and applicable law.	This clause is similar to the 'right to be forgotten' as prescribed under the PDPB, under S. 20(1)[15], and the right to erasure under S. 18(1)(d)[16]. However, considering that the bill is yet to be passed, adequate provisions prescribing obligations of service providers to comply with such requests from data principals need to be prescribed under the policy. These may pertain to the following: 1. Service providers to give justification to data principals for rejecting any request (S. 18(2)[17] of the bill). 2. Data fiduciaries to notify all relevant entities or individuals, in case a data principal opts-out of the NDHE, or de-links their personal data across data fiduciaries, or cancel their Health ID, or require the removal of any personal data linked with such ID to whom such personal data may have been disclosed. The repercussions of not honouring legitimate opt-out requests also need to be provided.
Creation of Health ID		
17.2	A data principal may create his/her own Health ID themselves in accordance with the procedure set out in paragraph 17.3 below, or through the	The policy may explicitly clarify the same would be generated at no cost, as mentioned in clause 18.2, for Health Practitioner ID. The policy may further clarify that each Health ID would be unique, and no single data principal would

[15] The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure— (a) has served the purpose for which it was collected or is no longer necessary for the purpose; (b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or (c) was made contrary to the provisions of this Act or any other law for the time being in force.

[16] The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to the erasure of personal data which is no longer necessary for the purpose for which it was processed.

[17] Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.

Clause	Issue	CUTS Remarks
	services of a data fiduciary in accordance with the procedure set out in paragraph 17.4 of this Policy.	be allowed to generate more than one Health ID, as mentioned in clause 18.4 for Health Practitioner ID,and under 21.3 for Health Facility ID.
Allocation of a Health Practitioner ID		
18.5	A Health Practitioner ID may be used to view the electronic health records of a data principal, subject to such consent being provided by the data principal and strictly in accordance with the terms of such consent, as set out above in this Policy.	Given that health practioners have access to data principal's health records (sensitive personal data), adequate provisions may be incorporated in the policy pertaining to maintain confidentiality of such data. Furthermore, select principles pertaining to accountability, purpose limitation etc. must also be applicable on health practioners as are for data fiduciaries, under clause 26.
Principle of non-exclusion for Health Practitioner ID		
19.1	The participation of the health practitioner in the NDHE as set out under this Policy shall be as per the policy stipulated by NHA in this regard.	As mentioned in clause 16.1 for data principals, the participation of the health practitioner in the NDHE may also be mentioned to be on a voluntary basis.
19.2	Every health practitioner shall have the option of opting-out of the NDHE, cancelling their Health Practitioner ID, and requiring the removal of any personal data linked with such ID in accordance with the terms of the Data Retention and Archival Policy and applicable law.	Health practitioners right to exercise the given options, must be treated at par with the same right available to data principals. Accordingly, the suggestions given for clause 16.2 hold good for this clause as well.
Allocation of Health Facility ID		
21.1	A health facility in India may request for the creation of a Health Facility ID at no cost, which shall be required to enable them to participate in the NDHE as set out under this Policy.	As mentioned previously for Health Practioner ID and Health ID, the same may be mentioned to be created on a voluntary basis.
Obligations of data fiduciaries in relation to processing of personal data		

Clause	Issue	CUTS Remarks
26.3	Privacy by design	The policy differentiates between a privacy policy and a privacy by design policy. This distinction was however not made under the PDPB. It is recommended that parity must be maintained between the two, to ensure regulatory harmonisation. The privacy by design policy required to be made under the clause, must also draw from relevant provisions of the PDPB, i.e. S. 22(1)(d)[18].
26.5	Purpose limitation	While the provision in the policy is compatible with S. 4[19] of the PDPB, it must also include principles laid under S. 5(b)[20] and S. 6[21] of the PDPB. Furthermore, CUTS privacy survey exposed the awareness gap, and capacity constraints of users, on issues related to privacy and data protection. Accordingly, mechanisms such as purpose limitation become extremely relevant for avoiding excessive processing of data by service providers. The policy/bill may mandate any processing of personal data to be compatible with the original purpose of processing. This will promote innovation without enhancing privacy risks.
Other provisions		
12, 14, 27 & 33	Provisions pertaining to Processing personal or sensitive personal data pertaining to a child; Rights of data principals; Reasonable Security Practices and Procedures; Data management by data processors; Data Protection Impact Assessment; Personal Data Breach and Incident Management etc.	Such issues have been covered under the PDPB, and may not be overlapped in this policy as well, unless for laying any sector specific provisions. Please refer CUTS Submission to the Joint Committee on The Personal Data Protection Bill, 2019, for suggestions pertaining to select such provisions. Available here.

[18] the legitimate interests of businesses including any innovation is achieved without compromising privacy interests

[19] No personal data shall be processed by any person, except for any specific, clear and lawful purpose.

[20] for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.

[21] The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

Clause	Issue	CUTS Remarks
Sharing of de-identified or anonymised data by data fiduciaries		
29.1 & 31.2	Data fiduciaries may make anonymised or de-identified data in an aggregated form available 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 NHA. A database or record of any data which has been processed under this Policy shall not be made public, unless such database or record is in an anonymised/de-identified and aggregated form and is processed in accordance with the terms specified in Paragraph 29.2 of this Policy.	The Report by the Committee of Experts on Non-Personal Data Governance Framework[22] had recognised that even after personal data is anonymised, the possibilities of harm to the data principals is not totally gone, as it is being increasingly recognised that no anonymisation technique provides perfect irreversibility. It further stated that potential harms could arise in terms of privacy violations arising from reidentification of anonymised data, or from the derivation of personally identifiable insights from non-personal data. It called for developing adequate measures to ensure that any data sharing framework does not dilute the protections afforded by the PDPB. The report also stated that data principals' consent must be secured for anonymisation and usage of this anonymized data while providing consent for collection and usage of his/her personal data. The report is still being deliberated upon. Accordingly, it is recommended that the Policy waits for the finalisation and operationalisation of the Non-Personal Data Governance Framework before delving into the issue of sharing of de-identified or anonymised data by data fiduciaries. This is also relevant for clause 31.2 of the policy. This gains more significance for health-related data, given that it is classified as sensitive personal data under the PDPB.
Grievance Redressal and Compliance		
32.2	Grievance redressal	CUTS' privacy survey had pointed out, that only a few users who experienced a personal data breach or a privacy violation, went on to complain about it. Users were also found to be unaware regarding the avenues of registering their

[22] https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf

Clause	Issue	CUTS Remarks
		grievances. The policy may introduce mediation mechanisms on the lines of CUTS Grahak Sahayta Kendra.[23]
32.3		No time limit has been prescribed by the policy at the level of the NDHM-DPO as well as the MoHFW to dispose of any complaints made by users, which may deter them from pursuing their complaints in case of delays in getting their grievances redressed. Also, no provision has been made by the bill, for the DPA to provide a reasoned order with respect to complaints filed by users. Informed by the Consumer Protection Act 2019, a timeline for not more than sixty days may be provided for resolutions of complaints at the level of the NDHM-DPO. For further details, please refer CUTS policy brief on 'Consumer Grievance Redressal', available here.

The Way Forward

CUTS' opines that a policy is no substitute for legislation, especially when it pertains to the fundamental right of privacy, and issues already being deliberated in dedicated legislations. Accordingly, it is recommended that the policy may wait till the passage of the PDPB, and finalisation of the Non-Personal Data Governance Framework, in order to ensure harmonisation of the said policy/legislations.

CUTS' looks forward to the MoHFW considering the proposed suggestions given above, and to assist the MoHFW in its endeavours to create a National Digital Health Ecosystem. For any clarifications/further details, please feel free to contact Amol Kulkarni (amk@cuts.org) and/or Sidharth Narayan (sid@cuts.org).

[23] https://cuts-cart.org/consumer-care-centre-grahak-sahayta-kendra/