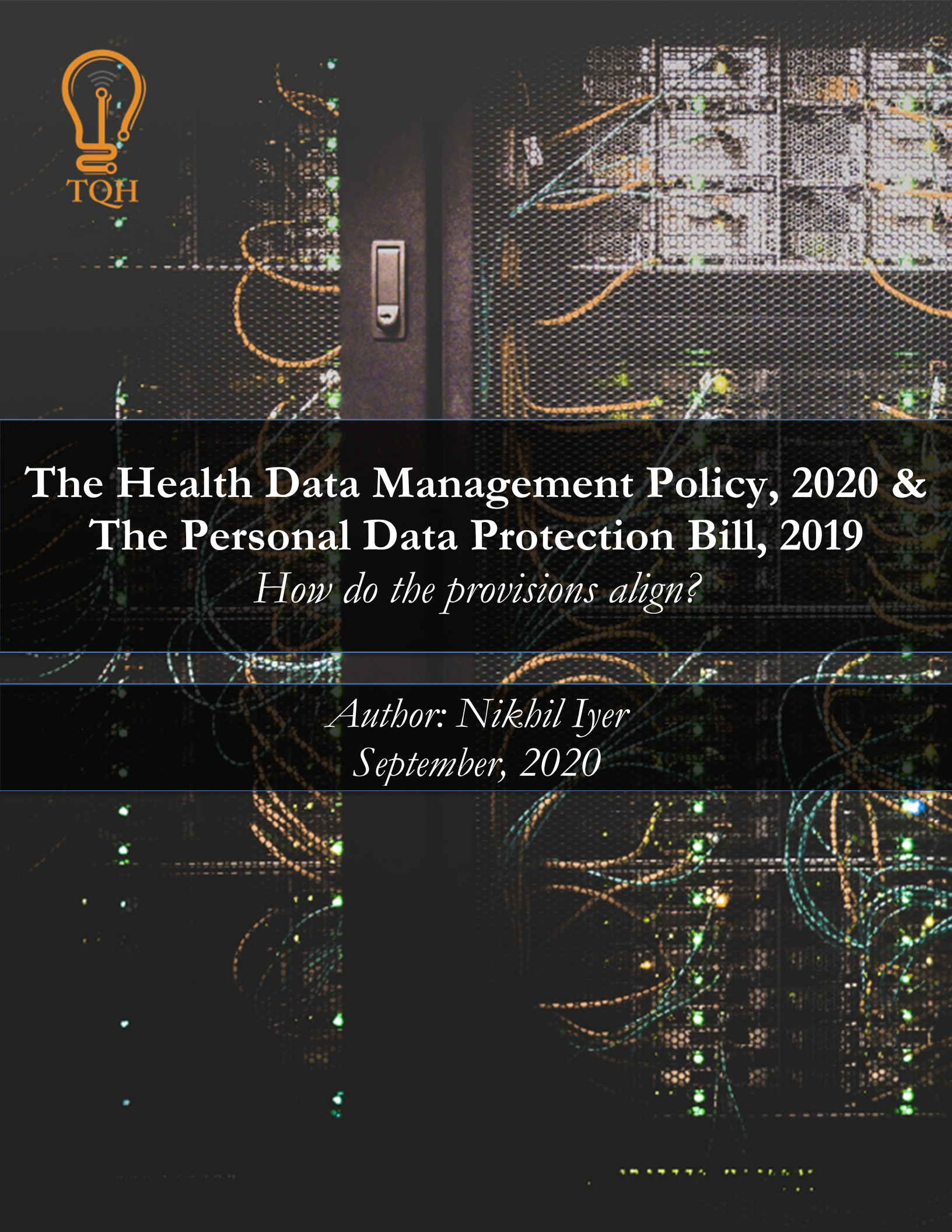

The Health Data Management Policy, 2020 & The Personal Data Protection Bill, 2019

How do the provisions align?

Author: Nikhil Iyer

September, 2020

The Ministry of Health of Family Welfare, Government of India circulated the 'Health Data Management Policy' (Policy Proposal hereafter) for feedback and consultation on 26th August 2020. This Policy Proposal will serve as the fulcrum for the National Digital Health Blueprint through which the government aims to build a 'federated' digital architecture to further the goals of the National Health Policy. The proposed digital architecture is expected to be available to all healthcare providers and users, as well as entities such as pharmaceutical and insurance companies.

The Policy Proposal is a 'guidance document' to regulate the vast amounts of data that will be generated and processed under this architecture. Admittedly, the driving force for the proposal is the necessity of safeguarding privacy of confidential health data. It seeks to build on the Personal Data Protection Bill, 2019 (PDP Bill, 2019), which is currently under consideration in Parliament. The utility of building a digital health ecosystem has long been accepted. Its benefits include improved access to health records across primary, secondary and tertiary healthcare, improved decision making for service delivery and research for innovative solutions. Both the Policy Proposal and the PDP Bill, 2019 aim to set out a legal framework against which entities in the health ecosystem may undertake such exercises.

The consultation process for the Policy Proposal is underway till 21st September, 2020. In this note, we analyse the key points of departure between the Policy Proposal and the Personal Data Protection Bill, 2019, with regard to three aspects:

1. Key Definitions
2. Consent Framework
3. Obligations on Data Fiduciaries

The Policy Proposal clarifies at the outset that no entity shall be entitled to any rights greater than what are already available under other applicable laws, which will presumably include the PDP Bill, 2019 and rules and regulations formed under this legislation once it is passed by Parliament. Readers can find a clause-by-clause comparison of the Policy Proposal and the PDP Bill, 2019 in the annexure to this note.

1. Key Definitions

a. Unique Identification: There is an overlap in the import of definitions of 'Biometric Data' and 'Personal Health Identifiers' as described below. Both describe unique identifiers by which one individual may be distinguished from another. Biometric Data is generally understood in the context of authentication and verification. Similarly, the Blueprint suggests that Personal Health Identifiers will be used in conjunction with Aadhar and other 'specified types of identifiers' to verify and allow access to Personal Health Lockers, which will readily give access to the person's health records.

   i. Biometric Data – This is defined as data that confirms the unique identification of a natural person. The PDP Bill includes facial images, fingerprints, and iris scans as biometric data. It also mentions other 'similar personal data' which may be measured or technically operated upon, which the Policy Proposal expands to include data on the physical, physiological, and behavioural characteristics. The inclusion of these characteristics is unique to the Policy Proposal and is not seen in either the PDP Bill or in other drafts on data protection released by the Government till now.

   ii. Personal Health Identifier (PHI) – The Policy Proposal alone mentions this. It refers to data that can be used to 'potentially identify a specific Data Principal' and distinguish such Data Principal from another. Even as PHIs may include a person's demographic and location information, family and relationship information and contact details, etc. the purpose of such data and that of Biometric Data is similar.

b. Profiling of Individuals: Inferences drawn for purposes of profiling are personal data under the PDP Bill, but not so under the Policy Proposal. Among other uses, profiling can be used to predict individual behaviour and offer goods or services they are likely to consume, through targeted advertising. In the health ecosystem, profiling will be relevant for offering a range of services, from diagnosis to medicines to health insurance. The change in the definition may mean that collection and storage of such data on profiling may not attract the compliances that other data within the definition would do. This is a matter of concern since patients and individuals requiring medical care may be especially vulnerable to profiling activities.

c. Re-Identification of Individuals: The definition of 'De-Identification', a process by which identifiers from personal data are removed or masked with other values or names, is the same under the Policy Proposal and the PDP Bill. Similarly, both documents forbid entities from knowingly or unknowingly re-identifying individuals from de-identified datasets. Nonetheless, the Policy Proposal mentions that Personal Health Identifiers can be used to re-identify persons. The Blueprint suggests that competent authorities may use PHIs for re-identification, for instance, to monitor spread of notified diseases, take timely decisions for public health, etc.

d. Anonymisation of Data: The PDP Bill, 2019 covers a range of operations such as collection, storage, retrieval, etc. in the ambit of 'Processing' of data. The Policy Proposal explicitly includes 'Anonymisation' within the meaning of 'Processing'. Further, in the PDP Bill, the standard for Anonymisation shall be set by the Data Protection Authority. On the contrary, the Policy Proposal

defines Anonymisation as a process by which the Data Principal cannot be identified by means 'reasonably likely to be used'. Even as commentators have highlighted that permanent anonymisation is nearly never possible, the modified definition will attract compliance provisions when anonymised data is shared for research purposes.

e. Sensitive Personal Data: Under both the Policy Proposal and the PDP Bill, certain data is classified as 'Sensitive Personal Data' owing to the nature of the information. It includes data relating to finances, health, sex life, genetics, caste, etc. of the individual. The Policy Proposal modifies the list of such data as follows:
   - Financial Data is to include bank account or payment instrument details.
   - Health Data is described as 'physical, physiological and mental health data'.
   - Sensitive Personal Data will include Medical Records and History, and information relating to health conditions and treatments, such as the Electronic Health Record, Electronic Medical Record, and Personal Health Record.

2. Consent Framework

a. Standard and Purpose of Consent: Consent, under both the PDP Bill, 2019 and this Policy Proposal, must be free, informed, specific, clear, and revocable. While both need individuals to be able to determine the scope of consent they have given, the Policy Proposal adds that consent must be given for a particular purpose. The requirement of the PDP Bill that consent should be clearly given (referring to an 'affirmative action that is meaningful in a given context') is removed from the Policy Proposal. This difference in the standard of consent may be particularly relevant in the health ecosystem. For instance, where medical emergencies may require time bound action (e.g. after a road accident), the hospital may not be in a position to obtain consent that may be strictly valid as per the PDP Bill. The patient may be unable to consent with 'affirmative action that is meaningful' at every stage of treatment. Nonetheless, since urgent medical care may be critical at that moment, the standard of consent has been slightly tweaked in the Policy Proposal.

   Crucially, the National Health Authority shall specify the purposes for which consent may be obtained in the health ecosystem.

b. Consent for Sensitive Personal Data: The PDP Bill explicitly prohibits obtaining consent by 'inference from conduct in a context' for sensitive personal data. In comparison, this Policy Proposal has no such prohibition. Moreover, it does not need the Data Fiduciary to give individuals the choice of separately consenting for use of different categories of Sensitive Personal Data. The previous analysis is applicable here as well, especially since data on medical records and history is sensitive personal data. Data Fiduciaries may be necessitated to infer consent from the patient's conduct, as compared to obtaining explicit and affirmative consent.

   The PDP Bill also allows for processing of Personal Data without consent if done in case of medical emergency relating to Data Principal or any other individual, to provide medical treatment or health service. This exception is available to data fiduciaries under the Policy Proposal as well.

c. Privacy Notice for Obtaining Consent: There are minor differences in the language used in the Policy Proposal and the PDP Bill. Privacy Notice under the PDP Bill must be given at the time of collection, or as soon as reasonably practicable where data is not collected from the Data Principal. Under the Policy Proposal, the Privacy Notice must be given prior to collection of Personal or Sensitive Personal Data, and each time when such collected data is processed for any new or previously unidentified purpose. The contents of the Privacy Notice that must be given to obtain consent are largely similar in the two documents. Three pieces of additional information must be provided under the provisions of the Policy Proposal. These are:

   i. The method or mechanism of data collection
   ii. The identity and contact details of the data fiduciary
   iii. The details of the mechanism for dealing with complaints, inquiries, practices and procedures regarding collection, storage, transmission, etc.

   Further, under the Policy Proposal, information regarding cross border transfer of personal data need not be included in the Privacy Notice. This is likely due to the Government's intention to mandate processing of health and medical data within India. The Policy Proposal also requires the Privacy Notice to be in as many languages in which a company (Data Fiduciary) intends to provide their service, which is in line with the requirement of informed consent.

d. Consent of Data Principals who are seriously ill or mentally incapacitated: The PDP Bill, 2019 has no specific provisions on Data Principals who are seriously ill or are mentally incapacitated. On the other hand, the Policy Proposal creates a nominee system, where a nominee of such Data Principal can consent on her behalf in case the Data Principal becomes seriously ill or is mentally incapacitated and is unable to give valid consent. Where no person has been nominated, any adult member of their family can perform this role. This is especially relevant in the health ecosystem, where Data Principals may often not be in a position to provide valid consent first-hand.

3. **Obligations on Data Fiduciaries**

a. Obligations similar to Significant Data Fiduciaries: The primary point of departure between the PDP Bill and the Policy Proposal is in imposition of obligations. All Data Fiduciaries in the digital health ecosystem have obligations similar to those of 'Significant Data Fiduciaries' under the PDP Bill, 2019. Under Section 26 of the PDP Bill, the Data Protection Authority may notify an entity as a Significant Data Fiduciary based on factors such as volume, sensitivity, or risk of harm from processing of personal data, etc. Such notification shall attract obligations of conducting Data Protection Impact Assessments, Maintenance of Records on Security Safeguards etc., and audits to be conducted by independent auditors. On the other hand, these obligations are applicable to all data fiduciaries under the Policy Proposal. This is a likely acknowledgment of the sensitivity of data that will be processed in the health ecosystem.

b. Data Principal's Right to Erasure: While the right to erasure exists under the PDP Bill as well, the Policy Proposal explicitly provides for erasure where the storage of Personal Data violates any data protection principles or if the original purpose for collection is satisfied. Further, where personal data

cannot be erased due to legal mandates or disproportionate effort on part of the data fiduciary, the Policy Proposal suggests that methods of over-writing, anonymisation, or other methods of removal of data from live systems be used. These alternatives are unique to the proposal.

c. Privacy Policy: In addition to the Privacy by Design Policy under the PDP Bill, the Policy Proposal mandates a 'Privacy Policy' to be published for public access by data fiduciaries. This would include types and purposes of data collected, whether it is being shared with other entities, and the security measures taken to safeguard such data. This requirement is also unique to the Policy Proposal.

d. Security Practices and Procedures: The Policy Proposal mandates a 'comprehensive documented information security programme' and an 'Information Security Policy'. Amongst other security measures mentioned in the PDP Bill, the Policy Proposal also states that data fiduciaries shall implement International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements". These requirements are specific to the health data ecosystem.

e. Data Processors: The PDP Bill necessitates that a contract must exist between the Data Fiduciary and the Data Processor before any processing activity is done. The Policy Proposal goes further to demand a due diligence check on the Data Processor, and the execution of confidentiality and non-disclosure agreements between the two parties. Further, data should be shared with Data Processors only on a 'need-to-know' basis.

f. Privacy Training and Awareness: The Policy Proposal mandates training and awareness programmes to be conducted by the Data Fiduciary for its own employees and for the Data Processors, at least once per year. It further suggests that attendance records be maintained for these sessions and reviewed during the audit process. No such obligation exists under the PDP Bill, 2019.

Annexure

1. **Key Definitions** (note: differences are highlighted in yellow)

Definition	Personal Data Protection Bill, 2019	Health Data Management Policy, 2020
Anonymisation	means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority	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
Biometric data	means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations	means facial image, fingerprint scans, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural characteristics of a data principal, which allow or confirm the unique identification of that natural person
Data	includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means	means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means
Data fiduciary	means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data	means any person, including the State, a company, any juristic entity or any individual who alone, or in conjunction with others, determines the purpose and means of processing of personal data. For the purpose of this Policy, data fiduciaries would include Health Information Providers and Health Information Users if such entities are determining the purpose and means of processing of personal data
Data Principal	means the natural person to whom the personal data relates	means the natural person/individuals to whom the personal data relates
Data processor	means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary	means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary
De-identification	means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace	means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or

	them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal	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
Electronic Health Records	-	are one or more repositories, physically or virtually integrated, of data in digital form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users (such as health practitioners or health facilities), represented according to a standardized or commonly agreed logical information model. Essentially, an EHR is a collection of various medical records that get generated during any clinical encounter or events;
Electronic Medical Records	-	refers to a repository of records that is stored and used by the HIP generating such records to support patient diagnosis and treatment. EMR may be considered as a special case of EHR, limited in scope to the medical domain or is focused on the medical transaction
Harm	Includes – 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.	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.

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	-
Information Security Policy	-	means the Information Security Policy which shall be formulated by the NHA
Personal data	means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling	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
Personal Health Identifier	-	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
Processing	in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction	in relation to personal data, means an operation or set of operations performed upon personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, anonymisation, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction
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
Re-identification	means the process by which a data fiduciary or data processor may reverse a process of de-identification	-
Repository	-	means a system where data is stored, maintained and preserved in a digital form and is optimised for various uses and functions, as may be required
Sensitive Personal Data	means such personal data, which may, reveal, be related to, or constitute — i. financial data; ii. health data; iii. official identifier; iv. sex life; v. sexual orientation vi. biometric data; vii. genetic data; viii. transgender status; ix. intersex status; x. caste or tribe; and xi. religious or political belief or affiliation xii. any other data categorised as sensitive personal data under Sec. 15.	means such personal data, which may reveal or be related to, but shall not be limited to, i. financial information such as bank account or credit card or debit card or other payment instrument details; ii. physical, physiological and mental health data; iii. sex life; iv. sexual orientation; v. medical records and history; vi. biometric data; vii. genetic data; viii. transgender status; ix. intersex status; x. caste or tribe; and xi. religious or political belief or affiliation For the purposes 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.
Significant Data Fiduciary	means a data fiduciary classified as such under sub-section (1) of section 26	-
Significant Harm	means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm	means harm that has an aggravated effect having regard to the nature of the personal data being processed, the impact, continuity, persistence or irreversibility of the harm

2. Consent Framework

Heading	Personal Data Protection Bill, 2019	Health Data Management Policy, 2020
Consent	Will not be considered valid unless it is: - Free (as under Sec. 14 of Indian Contract Act, 1872); - Informed (data principal must be provided information as required under Sec. 7 of the PDP Bill, 2019); - Specific (whether data principal can determine the scope of consent in respect of the purpose of processing); - Clear (whether indicated through an affirmative action that is meaningful in a given context); - Capable of being withdrawn (whether the ease of such withdrawal is comparable to the ease with which consent may be given). Consent in respect of sensitive personal data shall be explicitly obtained – a. after informing data principal of purpose of, or operation in, processing which is likely to cause significant harm to the data principal b. in clear terms without recourse to inference from conduct in a context c. after giving choice of separately consenting to purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing. Burden of proof that consent has been given by data principal for processing of personal data shall be on data fiduciary.	Will be considered valid only if it is: - Free (as under Sec. 14 of Indian Contract Act, 1872) - Informed (data principal must be provided necessary information as required under Para. 10 of the Policy, the scope of consent in respect of purpose of processing - Specific (consent given for processing of personal data for a particular purpose) - Clearly given - Capable of being withdrawn (whether the ease of such withdrawal is comparable to the ease with which consent may be given). Purposes for processing of personal data shall be limited to those as specified by the National Health Authority. The consent of a data principal in respect of collecting or processing any sensitive personal data will be obtained only after informing him/her the purpose of, or operations in, processing which are likely to cause significant harm to the data principal.
Privacy Notice by Data Fiduciaries	Notice must be given to data principal at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable,	Clear and conspicuous privacy notice must be given to data principals, a. Prior to collection of personal

	containing the following information – a. purposes for which the personal data is to be processed; b. nature and categories of personal being collected; c. identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable; d. the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent; e. the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds specified in sections 12 to 14; f. source of such collection, if the personal data is not collected from the data principal; g. individuals or entities including other data fiduciaries or data processors with whom personal data may be shared, if applicable; h. information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable; i. period for which the personal data shall be retained in terms of section 9 (restrictions on retention of personal data) or where such period is not known, the criteria for determining such period; j. the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same; k. procedure for grievance redressal under section 32; l. existence of a right to file complaints to the Authority; m. where applicable, any rating in the form of a data trust score that may be assigned to the data fiduciary under sub-section (5) of section 29; and	or sensitive personal data; b. At the time the data fiduciary changes its privacy policies or procedures; c. Prior to collection or further processing of personal or sensitive personal data of the data principal for any new or previously unidentified purpose. The notice should contain the following information – a. purposes for which the personal or sensitive personal data is to be processed; b. nature and categories of personal or sensitive personal data being collected by data fiduciary; c. methods or mechanisms by which the personal or sensitive personal data is collected by the data fiduciaries; d. identity and contact details of the data fiduciary collecting the personal or sensitive personal data; e. right of the data principal to withdraw her/his consent, and the procedure for such withdrawal; f. individuals or entities along with their contact details, including other data fiduciaries or data processors with whom personal or sensitive personal data may be shared, if applicable; g. period of time for which the personal or the sensitive personal data shall be retained, or where the period of retention is not known, then the criteria for determining such period; h. existence of and the procedure for the exercise of rights of the data principal as referred to in paragraph 14 of this Policy; and i. the contact details and the mechanism by which the data

	n. any other information as may be specified by the regulations. Privacy notice to be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.	principals may contact the data fiduciary in relation to complaints, inquiries, and clarifications regarding the policies, practices and procedures employed in the collection, storage, transmission or any other aspect of processing of personal or sensitive personal data. Privacy notice to be clear, concise and easily comprehensible to a reasonable person and available in as many languages in which the services of the data fiduciary are intended to be provided.
Processing data pertaining to a child	Before processing personal data, the data fiduciary shall verify the child's age and obtain consent of the parent or guardian. The verification of child's age shall be specified by regulations, based on volume of personal data processed, proportion of such personal data likely to be of the child, possibility of harm arising to the child, and other factors as prescribed. Where data fiduciary operates commercial websites or online services directed at children, or processes large volumes of personal data of children, they will be classified as 'guardian data fiduciary'. Such classification shall prohibit them from profiling, tracking or behaviourally monitoring or using targeted advertising on children.	Data fiduciary must obtain the consent of parents or guardians before data of the child is processed. Such processing should be in the best interests of the child and should not be in a manner that is likely to cause harm to the child. To verify the consent of the parent or guardian, a valid proof of relationship and proof of identity of parent is to be submitted to the data fiduciary.
Processing data of data principals who are seriously ill or mentally incapacitated	-	The National Data Health Ecosystem (NDHE) requires data principals to provide information about their nominees. Where a data principal becomes seriously ill or is mentally incapacitated and is unable to give valid consent, their nominee shall be authorised to give valid consent. In case no person has been nominated, any adult member of their family can give valid consent on their behalf. Such consent can be given only where there is proof of

		relationship, along with proof of medical condition of the data principal.

3. Obligations on Data Fiduciaries:

Right of data principals to	PDP Bill, 2019	Health Data Management Policy, 2020
Confirmation and Access	Similar provisions	Similar provisions
Correction and Erasure	Data principals may request data fiduciary to correct inaccurate or misleading personal data, complete the incomplete personal data, update out-of-date personal data, and erase personal data that is no longer necessary for the purpose for which it was processed. Where the data fiduciary does not agree with such a request, they shall provide adequate justification in writing to the data principal. If data principal is not satisfied by the justification, they may require the data fiduciary to take reasonable steps to indicate alongside the relevant personal data that such data is disputed.	Similar provision relating to rectification, completion and updation of personal data. Data principals can request for erasure where the storage of personal data violates any data protection principles or if the original purpose for collection has been satisfied. They can delete personal data in their health lockers unless storage is mandated by law. The policy suggests where personal data cannot be erased either due to legal mandates or involvement of disproportionate effort on part of data fiduciary, methods of over-writing, anonymisation or other methods of removal of data from live systems can be used. Disposal of any personal data shall be in accordance with law, rules, regulations, standards, this Policy, the Information Security Policy, and the Data Retention and Archival Policy. A certificate or other notification of the destruction may be required. The process of written justification in case of denial of request, and indication of 'disputed status' of data exist under this Policy too.
Data portability	Similar provisions	Similar provisions
Prohibit disclosure of personal data	The Bill provides the larger Right to be Forgotten to the data principal, for which an application must be made to the Adjudicating Officer.	The Policy states "Subject to applicable law, the data principal can restrict or object to the disclosure of their personal data by the data fiduciary."

The PDP Bill, 2019 and this Policy Proposal both impose similar obligations on data fiduciaries, premised on certain privacy principles.

Privacy Principle	Personal Data Protection Bill, 2019	Health Data Management Policy, 2020
Accountability	Similar provisions	Similar provisions
Transparency	Similar provisions	Similar provisions
Privacy by Design	Similar provisions on Privacy by Design Policy to be published by the data fiduciary.	In addition to the Privacy by Design Policy, the Health Data Management Policy, 2020 states that data fiduciaries must also prepare a 'Privacy Policy' containing the following – a. Clear and easily accessible statements of its practices and policies; b. type of personal or sensitive personal data collected; c. the purpose of collection and usage of such personal or sensitive personal data; d. whether personal or sensitive personal data is being shared with other data fiduciaries or data processors; e. reasonable security practices and procedures used by the data fiduciary to safeguard the personal or sensitive personal data that is being processed.
Consent Driven Sharing	Similar provisions	Similar provisions
Purpose Limitation	Similar provisions	Similar provisions
Collection, Use and Storage Limitation	Similar provisions	Similar provisions
Empowerment of Data Principal	Similar provisions	Similar provisions
Data Quality	Similar provisions	Similar provisions
Security Practices and Procedures		
Reasonable Security Practices and Procedures	Data fiduciary and data processor shall implement necessary security safeguards including methods of de-identification and encryption, steps to protect integrity of	This Policy imposes certain additional requirements – a. Data fiduciaries are required to

	personal data, and to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data. There must be periodic review of these security safeguards as specified by regulations.	have a comprehensive documented information security programme and Information Security Policy that have managerial, technical, operational and physical security measures commensurate with data being protected by them. b. In case of a data breach, data fiduciary may be called upon by an agency under law to demonstrate that they have implemented measures as per their documented Information Security programme and policies. c. The data fiduciaries will implement the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" as well as any other standard as may be applicable to them. At least once a year or as and when there is significant upgradation of a data fiduciary's processes, resources or systems, an independent auditor duly approved by the Central Government shall certify or audit on a regular basis the standards adopted for security practices and procedures.
Data Management by Data Processors		
Data Processors	The PDP Bill, 2019 mandates the existence of a contract between the data fiduciary and data processor before any data is processed by the latter.	In addition to the requirement of a contract, the Policy requires data fiduciaries to conduct appropriate due diligence covering data privacy and security prior to engaging with any data processor. Further, confidentiality agreements and non-disclosure agreements must also be executed between these parties. Data fiduciaries should ensure access to personal data for data processors must be

		on a 'need-to-know' basis. The data processor may not involve any other data processor unless authorised and permitted by the data fiduciary in their contract for engagement. Data fiduciaries must provide data privacy training and awareness programs on a periodic basis (at a minimum on an annual basis) for all employees and data processors. Attendance records for such training shall be maintained for documentation and audit purpose.