National Digital Health Mission: Health Data Management Policy

Chapter I: Preliminary

1. Purpose

The Ministry of Health and Family Welfare ("**MoHFW**") is responsible for conceiving the idea of the National Digital Health Mission ("**NDHM**"). This visionary project of the Government of India, stemming from the National Health Policy, 2017 ("**National Health Policy**") intends to digitise the entire healthcare ecosystem of India. This would be done by creating digital health records and creating and maintaining registries for healthcare professionals and health facilities in order to ensure a smooth interoperable framework for the multiple partners associated with healthcare delivery to individuals in India. The National Digital Health Blueprint, 2019 (the "**Blueprint**") recommends that a federated architecture be adopted, instead of a centralised architecture for the management of health data to ensure interoperability, technological flexibility and independence across the National Digital Health Ecosystem ("**NDHE**"). The data collected across NDHE will be stored at three levels, *i.e.* at a Central level, at a State or Union Territory level and lastly, at the health facility level, adopting the principle of minimality at each level. The federated structure necessitates the development of a framework that can be utilised throughout the NDHE to safeguard the privacy of confidential health data that has been collected from individuals in India. This would be essential to build a trust quotient across the NDHE as well as to ensure that the personal and health data of all individuals in India is adequately protected.

To that end, this Health Data Management Policy (the "**Policy**") is the first step in realising NDHM's guiding principle of "Security and Privacy by Design" for the protection of individuals' data privacy. It acts as a guidance document across the NDHE and sets out the minimum standard for data privacy protection that should be followed across the board in order to ensure compliance with relevant and applicable laws, rules and regulations.

This Policy is to be read along with, and not in contradiction to, any applicable law, or any instrument having the effect of any law together with the Blueprint, the information security policy, the data retention and archival policy and any other policy which may be issued for the implementation of the NDHM. This Policy is not to be interpreted or construed as giving any entity or individual rights which are greater than those that such entity or individual would be entitled to under applicable laws.

2. Applicability

The provisions of this Policy shall be applicable to the entities involved in the NDHM and the partners/persons who are a part of the NDHE. This includes:

(a) All entities and individuals who have been issued an ID under this Policy;

(b) healthcare professionals, including but not limited to doctors or health practitioners, nurses, laboratory technicians, and other healthcare workers;

(c) governing bodies of the MoHFW, the National Health Authority ("**NHA**"), relevant professional bodies and regulators;

(d) Health Information Providers;

(e) any health care provider who collects, stores and transmits health data in electronic form in connection with its transactions;

(f) payers i.e., Central Government, State Governments, insurers, health plans, charitable institutions, etc.;

(g) pharmaceuticals – drug manufacturers, medical device manufacturers, and entities involved in the relevant supply chain;

(h) research bodies – institutions, individual researchers including researchers utilising data for health data analytics, statisticians, analysts, public health institutions, etc.;

(i) Health ID holders i.e., patients, family members and beneficiaries;

(j) all individuals, teams, entities or ecosystem partners who collect or process personal or sensitive personal data of any individual as part of the NDHE; and

(k) all methods of contact, including in person, written, via Internet, direct mail, telephone or facsimile, as the case may be.

3. Objectives

The key objectives of this Policy are:

(a) to provide adequate guidance and to set out a framework for the secure processing of personal and sensitive personal data of individuals who are a part of the NDHE in compliance with all applicable laws;

(b) to safeguard digital personal health data, including the Personal Health Identifier, the electronic health records and electronic medical records, by implementing adequate technical and organisational measures across the NDHE ecosystem;

(c) to create a system of digital personal and medical health records which is easily accessible to individuals and health service providers and is purely voluntary in nature, based on the consent of individuals, and in compliance with international standards such as ISO/TS 17975:2015 (defines the set of frameworks of consent for the collection and processing of health data by healthcare practitioners and other entities) and other relevant standards related to data interoperability and data sharing as may be notified for the implementation of NDHM from time to time;

(d) to increase awareness of the importance of data privacy and instil a privacy-oriented mindset among the members of NDHM and its ecosystem partners;

(e) to ensure national portability in the provision of health services;

(f) to establish appropriate institutional mechanisms for auditing of the NDHE as needed and to encourage stakeholders and ecosystem partners to adopt the data protection principles set out in this Policy; and

(g) to leverage the information systems existing in the Indian health sector by encouraging conformity with the defined data privacy standards and integrating such existing systems with NDHE.

4. Definitions

In this Policy, unless the context otherwise requires, -

(a) “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;

(b) “biometric data” 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;

(c) “child” means a natural person/individual who has not completed eighteen years of age;

(d) “consent” means the consent referred to in paragraph 9 of this Policy;

(e) “consent artifact” means a machine-readable document that specifies the parameters and scope of data sharing and access that a data principal consents to in any personal data sharing transaction;

(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;

(g) “data” 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;

(h) “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. 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;

(i) “data principal” means the natural person/individual to whom the personal data relates;

(j) “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;

(k) “Data Retention and Archival Policy” means the Data Retention and Archival Policy which shall be formulated by the NHA;

(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;

(m) “electronic health records” or “EHR” 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;

(n) “electronic medical records” or “EMR” 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;

(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;

(p) "health facility" refers to health facilities across the country such as hospitals, clinics, diagnostic centres, health and wellness centres, mobile vans, ambulances, pharmacies etc.;

(q) "Health Facility ID" refers to the unique ID allocated to each health facility in accordance with Chapter IV of this Policy;

(r) "Health ID" refers to the Identification Number or Identifier allocated to a data principal in accordance with Chapter IV of this Policy;

(s) "Health Information Provider" or "HIPs" means hospitals, diagnostic centres, public health programs or other such entities registered with the National Health Infrastructure Registry, which act as information providers (by generating, storing and distributing health records) in the digital health ecosystem. The NHA may, from time to time, specify certain terms and conditions in relation to HIPs;

(t) "Health Information Users" or "HIUs" are entities that are permitted to request access to the 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;

(u) "health locker" means a service of information exchange of electronic health records or electronic medical records, which can be accessed by the data fiduciary or data processor upon receiving the consent of the data principal and where such service can also be used by a data principal in order to create Personal Health Records;

(v) "Health Practitioner ID" refers to the unique ID allocated to each health practitioner in accordance with Chapter IV of this Policy;

(w) "Information Security Policy" means the Information Security Policy which shall be formulated by the NHA;

(x) "NHIR" refers to the National Health Infrastructure Registry;

(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;

(z) “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;

(aa) “Personal Health Records” or “PHR” is a health record that is initiated and maintained by an individual. An ideal PHR would provide a complete and accurate summary of the health and medical history of an individual by gathering data from many sources and making this accessible online. Generally, such records are maintained in a secure and confidential environment such as in a health locker, allowing only the individual, or people authorized by the individual, to access the medical data;

(bb) “processing” 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;

(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;

(dd) “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;

(ee) "sensitive personal data" means such personal data, which may reveal or be related to, but shall not be limited to,

(i) financial information such as bank account or credit card or debit card or other payment instrument details;
(ii) physical, physiological and mental health data;
(iii) sex life;
(iv) sexual orientation;
(v) medical records and history;
(vi) biometric data;
(vii) genetic data;
(viii) transgender status;
(ix) intersex status;
(x) caste or tribe; and
(xi) religious or political belief or affiliation.

For the purpose of this Policy, sensitive personal data would include information relating to various health conditions and treatments of the data principal, such as EMR, EHR and PHR; and

(ff) “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.

Chapter II: Applicable Law and Governance Structure

5. Applicable laws and regulations

Data fiduciaries must adhere to and comply with all applicable laws, and rules and regulations made thereunder, and any other standards pertaining to data protection, processing of personal or sensitive personal data, informational privacy, and information technology that may currently be in force in India.

6. Governance structure

The governance structure for the NDHE shall be as specified by the NHA, which shall lead the implementation of the NDHM. In addition, the governance structure shall consist of such committees, authorities and officers at the national, state and health facility levels as will be necessary to implement the NDHM. It shall also consist of a data protection officer ("**NDHM-DPO**") who shall be a government officer and who shall, in addition to the functions identified under this Policy, 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. It is envisaged that the MoHFW and the Ministry of Electronics and Information Technology ("**MeitY**") shall also provide overall guidance to the NHA on relevant aspects of the NDHM. Further specific details in relation to governance structure may be stipulated from time to time.

Chapter III: Consent Framework

7. Collection of personal or sensitive personal data by data fiduciaries

Data fiduciaries can collect personal or sensitive personal data in accordance with this Policy.

8. General principles governing consent framework

The consent framework under this Policy should incorporate the following principles in relation to processing of personal or sensitive personal data of data fiduciaries:

(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.

(b) Specifically, in case of electronic consent, data fiduciaries should make use of appropriate technological means to prevent security breaches and to guarantee integrity of access permissions given by data principals. Such technological means must be in conformance with the national and international standards, as may be applicable.

(c) So far as sharing or disclosure of any personal or sensitive personal data is concerned, the technical design of the consent management framework should also ensure interoperability across all players of the NDHE. The framework should be agnostic to applications, programming languages, and platforms.

9. Consent in relation to collection and processing of personal or sensitive personal data

9.1 Data fiduciaries can collect or process personal or sensitive personal data only with the consent of the data principal. It is the responsibility of the data fiduciary to ensure that the consent given by the data principal is valid.

9.2 The consent of the data principal will be considered valid only if it is:

(a) free, having regard to whether it complies with the standards set out under Section 14 of the Indian Contract Act, 1872;
(b) informed, having regard to whether the data principal has been provided with the necessary information by way of notice, as set out in paragraph 10 of this Policy, the scope of consent in respect of the purpose of processing;
(c) specific, where the data principal can give consent for the processing of personal data for a particular purpose;
(d) clearly given; and
(e) capable of being withdrawn at any time, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

9.3 It is clarified that the purposes for processing of personal data as set out in paragraph 9.2 (b) above shall be limited to those as may be specified by the NHA.

9.4 In addition to the conditions mentioned in paragraph 9.2 above, the consent of a data principal in respect of collecting or processing any sensitive personal data will be obtained only after informing her/him the purpose of, or operations in, processing which are likely to cause significant harm to the data principal.

10. Privacy Notice for the collection of personal and sensitive personal data

10.1 All data fiduciaries must give a clear and conspicuous privacy notice to data principals,
(a) prior to the collection of personal or sensitive personal data from the data principal;
(b) at the time the data fiduciary changes its privacy policies or procedures; and
(c) prior to the collection or further processing of personal or sensitive personal data of the data principal for any new or previously unidentified purpose.

10.2 It is clarified that for the purpose of paragraphs 10.1(b) and (c) above, all data fiduciaries must obtain fresh consent from the data principal in accordance with Chapter III of this Policy.

10.3 The privacy notice should contain the following information:
(a) the purposes for which the personal or sensitive personal data is to be processed;
(b) the nature and categories of personal or sensitive personal data being collected by data fiduciary;
(c) the methods or mechanisms by which the personal or sensitive personal data is collected by the data fiduciaries;
(d) the identity and contact details of the data fiduciary collecting the personal or sensitive personal data;
(e) the right of the data principal to withdraw her/his consent, and the procedure for such withdrawal;
(f) the 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) the 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) the 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 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.

10.4 The privacy notice shall be clear, concise and easily comprehensible to a reasonable person and shall be available in as many languages in which the services of the data fiduciary are intended to be provided.

11. **Method of obtaining consent**

11.1 The consent of the data principal, as referred to in paragraphs 8 and 9 of this Policy, for collection, or further processing of personal or sensitive personal data, may be obtained electronically or physically on paper, either directly from the data principal or through a consent manager, as the case may be. Where the consent is received physically on paper, then such consent may be converted to electronic form by the consent manager or the data fiduciary. Where the data principal has revoked her/his consent, it shall be the duty of the consent manager to notify the data fiduciary of such revocation, as applicable.

11.2 It is clarified that electronic consent is the digital equivalent of a physical letter of permission given by the data principal which, when presented, allows the consent manager or the data fiduciary to collect the personal or sensitive personal data, or further process the personal or sensitive personal data that has already been collected from the data principal for a particular purpose, as the case may be.

11.3 So far as further processing of personal or sensitive personal data pursuant to paragraphs 11.1 and 11.2 above is concerned, the data principal provides consent for data access and sharing that takes place between the Health Information Providers and Health Information Users. If such processing is done through electronic consent, then a consent artifact is generated to initiate the sharing of personal data or sensitive personal data. The consent artifact will then be shared between the data principal and the Health Information Provider or a Health Information User, through a consent manager.

11.4 Subject to the provisions of applicable law and this Policy, NHA may further set out guidelines, technical specifications, etc. in relation to consent obtained by data fiduciaries for collection and further processing of personal or sensitive personal data of data principals.

12. Processing personal or sensitive personal data pertaining to a child

12.1 Data fiduciaries should ensure that the processing of the personal or sensitive personal data of a child takes place only in such manner that is in the best interests of the child.

12.2 Data fiduciaries should obtain the consent of the parents or guardians of the child prior to processing the personal or sensitive personal data of the child.

12.3 A valid proof of relationship and proof of identity of the parent is required to be submitted to the data fiduciary in order to verify the consent of the parent or guardian for processing the personal or sensitive personal data of the child as set out in paragraph 12.2 above.

12.4 Where the data fiduciary is processing the personal or sensitive personal data of a child, then they shall not process such personal or sensitive personal data in a manner that is likely to cause harm to the child.

13. Processing personal or sensitive personal data of data principals who are seriously ill or mentally incapacitated

13.1 At the time a data principal opts to participate in the NDHE framework, such data principal should name an individual who has attained the age of majority to act as the nominee of the data principal.

13.2 The individual who has been nominated as per paragraph 13.1 above will be authorised to give valid consent on behalf of the data principal in the event the data principal becomes seriously ill or mentally incapacitated and is unable to give valid consent.

13.3 In the event that the data principal has not nominated an individual as under paragraph 13.1 above, then any adult member of the family of the data principal can give valid consent on behalf of the data principal.

13.4 Consent can be given by a member of the family of the data principal as set out in paragraph 13.3 above only where there is proof of relationship, along with proof of medical condition of the data principal.

14. Rights of data principals

14.1 Data principals can request the following from the data fiduciaries:

(a) Confirmation and access:

(i) The data principal can obtain from the data fiduciary the following information:

- a confirmation as to whether it has processed any personal data of the data principal;
- the personal data that has been processed or a summary of the same;
- summary of processing activities carried out on such personal data; and
- any information provided under the notice issued in accordance with paragraph 10 of this Policy in relation to such processing.

(ii) The data fiduciary will provide the information under sub-clause (i) above in a clear and concise manner that is comprehensible to a reasonable person.

(iii) The data principal shall also have the right to access in one place the identities of all the data fiduciaries with whom her/his personal data has been shared by any data fiduciary together with the categories of personal data that has been shared.

(b) Correction and erasure:

(i) The data principal can, having regard to the purposes for which her/his personal data is processed, rectify any inaccurate or misleading personal data, complete any incomplete personal data and update any out-of-date personal data.

(ii) The data principal can request that their personal data be erased in certain circumstances:

- If the storage of the personal data violates any of the data protection principles or the purpose for which it was originally collected has been satisfied.

- Data principals can also delete the uploaded personal data stored in their health lockers.

- If the storage of the personal data for a certain period of time is mandated by law, it cannot be erased.

- Personal data can be blocked and restricted, rather than erased, insofar as the law prohibits erasure as it would impair legitimate interests of the data principal, or if the data principal disputes that the personal data is correct, and it cannot be ascertained whether they are correct or incorrect.

- Where erasure is not possible without disproportionate effort due to the specific type of storage, over-writing, anonymisation or other method(s) of removal of the personal data from live systems can be used.

- Disposal of any personal data will be handled with utmost care, in accordance with applicable law, rules, regulations, standards, this Policy, the Information Security Policy, and the Data Retention and Archival Policy. Where data processors are disposing of any personal data on behalf of the data fiduciary, a certificate or other notification of the destruction may be required.

(c) Restrict or object to disclosure: Subject to applicable law, the data principal can restrict or object to the disclosure of their personal data by the data fiduciary.

(d) Data portability: As may be applicable, the data principal can request a copy of the following in a structured, commonly used and machine-readable format, to the extent technically feasible from the data fiduciary:
   (i) the personal data provided to the data fiduciary;
   (ii) the personal data which has been generated in the course of provision of services by the data fiduciary; or
   (iii) the personal data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained.

   The data principal can also request that the personal data specified above be transferred to another data fiduciary.

14.2 General conditions for submitting requests

(a) All requests under paragraph 14.1 above will be made by the data principal in writing, through e-mail or any other electronic means to the designated officer of the data fiduciary either directly or indirectly through a consent manager.

(b) The request will be made with the necessary information as regards to the identity of the data principal and the data fiduciary will acknowledge the receipt of such request. All requests will be addressed by the data fiduciary in a timely manner and in compliance with the applicable laws, regulations and this Policy.

(c) In the event that any request for correction, completion, updation or erasure of any personal data is accepted by the data fiduciary, such data fiduciary will take necessary steps to notify all relevant

entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

(d) In the event that any request for correction, updation, completion or erasure of personal data is rejected, the data fiduciary will provide the data principal reasons in writing for such refusal. If the data principal is not satisfied with such reasons, it may require that the data fiduciary take reasonable steps to indicate, alongside the relevant personal data, that the same is disputed by the data principal.

(e) In the event of the death of the data principal, the legal heirs or representative of such data principal may have access to the personal data owned by the data principal, only if such access was consented to by the data principal.

(f) The data fiduciary will not impose any restrictions on the method and channel of raising requests by data principals under paragraph 14.1 above.

(g) The data fiduciary will maintain records of all requests received under paragraph 14.1 above irrespective of their fulfilling status.

Chapter IV: ID Policy

15. Allocation of Health ID

15.1 A data principal may request for the creation of a Health ID at no cost, which will be required to enable them to participate in the NDHE ecosystem. Any processing of personal data that may take place for creation of such ID must be in accordance with this Policy.

15.2 A Health ID may be generated through such means as may be specified by the NHA, and may be authenticated using a data principal's Aadhar number or any other document of identification as may be specified by the NHA.

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.

15.4 The consent given by a data principal shall be linked to his/her Health ID, and every such instance of consent given by a data principal shall also be accessible by the data principal through his/her Health ID.

15.5 A data principal in possession of a Health ID shall be able to provide or revoke his/her consent in order to enable or restrict any sharing of personal data linked with such ID, and shall be able to update his/her personal data in accordance with this Policy.

15.6 The NHA shall make reasonable efforts to ensure that the personal data of a data principal is linked to one Health ID to ensure continuity of records for such data principal, notwithstanding whether multiple Health ID's have been created for such data principal in the course of receiving any service or otherwise.

15.7 In the instance that a data principal in possession of a Health ID is unable to access personal data linked with such ID due to any reason, such as having previously opted-out of the NDHE or being unable to

provide details of such Health ID, the data principal shall be able to recover such data by authenticating their identity through such means as may be specified by the NHA.

16. Principle of non-exclusion for Health ID

16.1 The participation of the data principal in the NDHE as set out under this Policy shall be on a voluntary basis only.

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.

16.3 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.

16.4 It is clarified that no individual shall be denied access to any health facility or service, or any other right in any way merely by reason of not being in possession of a Health ID or for not opting to participate in the NDHE.

17. Creation of Health ID

17.1 A data fiduciary wishing to issue a Health ID can register with the NHA and obtain an authorisation key to access the services required for generation of a 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 services of a data fiduciary in accordance with the procedure set out in paragraph 17.4 of this Policy.

17.3 A data principal may create his/her Health ID by:

(a) accessing such web-based portal as may be specified by the NHA;
(b) authenticating his/her identity through Aadhar or other means as may be specified by the NHA;
(c) filling in the other details that are required on such portal; and
(d) enrolling for a Health ID.

17.4 A Health ID may be created for a data principal through the services of data fiduciary authorised by the NHA for the purpose of generating such ID. Such data fiduciary:

(a) shall verify whether a Health ID is linked to the Aadhar number of such data principal, if provided by the data principal;
(b) if no such ID exists, then the data fiduciary shall register such data principal and create his/her Health ID using Aadhaar authentication or other means of authentication as may be specified by the NHA; and
(c) may provide an e-card or a physical card ~~printout~~ to the data principal to enable them access to the details of their Health ID.

18. Allocation of a Health Practitioner ID

18.1 The processing of personal data for the creation of a Health Practitioner ID must be in accordance with the data protection principles set out in this Policy.

18.2 A health practitioner may request for the creation of a Health Practitioner ID at no cost, which will be required to enable them to participate in the NDHE as set out under this Policy.

18.3 A Health Practitioner ID may be generated through such means as may be specified by the NHA.

18.4 A Health Practitioner ID shall be in electronic form, and a health practitioner in possession of a Health Practitioner ID shall not be permitted to create a second ID. Such Health Practitioner ID shall be non-transferrable.

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.

18.6 A health practitioner may e-sign documents, such as e-prescriptions, diagnostic reports, discharge summaries and e-claims using their Health Practitioner ID.

18.7 A Health Practitioner ID shall be used to authenticate a health practitioner for services created by the NHA as part of the NDHE, including the purchase of liability insurance, tele-medicine and other government services.

19. 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.

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.

19.3. It is clarified that the right of a qualified health practitioner to practice or work in India shall not, in any way, be restricted or impeded merely by reason of not being in possession of a Health Practitioner ID or for not opting to participate in the NDHE.

20. Creation of Health Practitioner ID

20.1 A health practitioner shall be required to authenticate their professional credentials, and any updates to such credentials, through the respective council, board, department or regulatory or professional body which governs their practice in order to create a valid Health Practitioner ID.

20.2 The NHA shall specify the authorised registrars for the purpose of authentication of professional credentials as per paragraph 20.1 above.

20.3 A health practitioner may create their Health Practitioner ID by:

(a) accessing the web portal as may be specified by the NHA;
(b) authenticating their identity through Aadhar or other identity proof as may be specified by NHA;

(c) authenticating their professional credentials through the authorised registrars as under paragraph 20.2;
(d) filling in other details as may be required; and
(e) enrolling for the Health Practitioner ID.

21. 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.

21.2 A Health Facility ID may be generated through such means as may be specified by the NHA.

21.3 A Health Facility ID shall be in electronic form, and a health facility in possession of a Health Facility ID shall not be permitted to create a second ID.

21.4 A health facility in possession of a Health Facility ID may share the personal data of a data principal with such data principal and any health practitioners, subject to the consent of the data principal and in strict accordance with the terms of such consent, in accordance with this Policy.

21.5 The Health Facility ID may be used to e-sign all documents which are necessary to avail online services.

21.6 The possession of a Health Facility ID does not deem that the health facility is legal, or that it holds all permissions and licenses as may be required by applicable laws.

22. Principle of non-exclusion for Health Facility ID

22.1 The participation of the health facility in the NDHE as set out under this Policy shall be as per the policy stipulated by NHA in this regard.

22.2 Every health facility shall have the option of opting-out of the NDHE, cancelling their Health Facility 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.

22.3 The right of a health facility to provide any services in India shall not, in any way, be restricted or impeded merely by reason of not being in possession of a Health Facility ID or for not opting to participate in the NDHE.

23. Creation of Health Facility ID

23.1 A health facility may register their facility for a Health Facility ID as per the registration procedure as may be specified by the NHA.

23.2 The owner or manager of a health facility may update details of such facility through the web portal as may be specified by the NHA.

23.3 The owner or manager of a health facility referred to in paragraph 23.2 above is not deemed to be the true legal owner or manager of such health facility.

23.4 Any updates made under paragraph 23.2 above shall be verified by health facility auditors referred to in paragraph 24.2 below before confirmation in the NHIR.

24. National Health Infrastructure Registry

24.1 A health facility possessing a Health Facility ID shall be included as part of the NHIR.

24.2 THE NHIR shall deploy health facility auditors to verify that the services offered by the health facility are the same as claimed by such facility during the registration process, that such health facility is operational at the time of its listing and is located at the address as claimed by such health facility.

24.3 The NHIR shall authenticate that the person claiming to be the owner or manager of a health facility is capable of updating and maintaining the details of the facility online, and of e-signing digital documents on behalf of the health facility.

25. Safeguards for creation of Health ID, Health Practitioner ID or Health Facility ID

25.1 The processing of any personal data for the purpose of creating a Health ID, Health Practitioner ID or a Health Facility ID shall be in accordance with applicable law and the principles set out under this Policy.

25.2 The creation of a Health ID, Health Practitioner ID or Health Facility ID shall collect only such data as may be essential to identify and authenticate a data principal, health practitioner or health facility, as the case may be, and any personal or sensitive personal data which is not essential for this purpose shall not be processed for the purpose of creating such ID.

Chapter V: Obligations of data fiduciaries in relation to processing of personal data

26. Privacy principles to be followed by data fiduciaries

Subject always to the provisions of applicable laws, data fiduciaries will follow the following principles while processing any personal data under this Policy:

26.1 Accountability

They will be accountable for complying with measures which give effect to the privacy principles while processing any personal data by it or on its behalf. However, the true ownership and control of the personal data will remain with data principals.

26.2 Transparency

They will take all necessary steps to maintain transparency in processing any personal data and will make the following information available:

(a) the categories of personal data generally collected and the manner of such collection;
(b) the purposes for which the personal data is generally processed;
(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
(d) the existence of and the procedure for exercise of rights of data principal and any related contact details for the same;
(e) the grievance redressal procedure; and

(f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary.

In addition to the information specified above, the data fiduciary will also notify the data principal, from time to time, the important operations in the processing of any personal data related to the data principal. The information provided by the data fiduciary will be in an intelligible form, using clear and plain language

26.3 Privacy by Design

They shall consider data protection requirements as part of the design and implementation of their systems, services, products and business practices. The federated design of the NDHE ensures personal data of the data principals will be held at the point of care or at the closest possible location where it was created, with no centralised repository. As such, data storage shall incorporate privacy control and safeguards right from the foundational levels.

They will prepare a privacy policy containing the following information:

(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.

The privacy policy referred to above shall be published on the website of the data fiduciary. In addition, they shall also make available a privacy by design policy on its website containing the following information:

(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
(b) the obligations of data fiduciaries;
(c) the technology used in the processing of personal data, in accordance with commercially accepted or certified standards;
(d) the protection of privacy throughout processing from the point of collection to deletion of personal data;
(e) the processing of personal data in a transparent manner; and
(f) the fact that the interest of the data principal is accounted for at every stage of processing of personal data.

26.4 Choice and Consent Driven Sharing

They will give data principals a choice to opt-in/opt out of the NDHE and take their consent in accordance with paragraph 9 of this Policy prior to accessing, sharing or processing any of their personal data. This consent will be free, informed, clear and specific in respect of the purpose identified in the privacy notice issued under paragraph 10 of this Policy.

26.5 Purpose Limitation

All personal data collected and processed by the data fiduciaries should be for a specific, lawful and clear purpose identified in the privacy notice issued under paragraph 10 of this Policy and consented by the data principal.

26.6 Collection, Use and Storage Limitation

They will collect the personal data from the data principals as is necessary for the purposes of processing and will use the personal data for the purpose for which it was collected. The processing of all personal data will be in a fair and reasonable manner, ensuring the privacy of the data principal. No personal data shall be transferred by the data fiduciary unless such transfer is in accordance with this Policy, subject always to the provisions of applicable laws. The personal data collected will not be retained beyond the period necessary to satisfy the purpose for which it is collected and the data fiduciary will delete such personal data at the end of such processing in accordance with paragraph 14 of this Policy as well as the Data Retention and Archival Policy. Personal data may be retained for a longer period of time if explicitly consented to by the data principal or if such retention is necessary to comply with any obligation under any applicable law. The data fiduciary will undertake a periodic review to determine whether it is necessary to retain the personal data in its possession.

26.7 Empowerment of Data Principal

The data fiduciary should believe in strengthening the rights of data principals in relation to their personal data. Data principals will enjoy rights as specified in paragraph 14.1 of this Policy.

26.8 Data Quality

They shall take necessary steps so that the personal data which is processed is updated, complete, accurate, and not misleading, having regard to the purpose for which it is processed. All personal data should be reliable and verifiable. However, the data fiduciary will not be responsible for the authenticity of the personal data supplied to them by the data principal.

Personal data once created cannot be deleted or amended without following the due process referred to in paragraph 14.2 of this Policy. All personal data must also be traceable to its creator unambiguously.

26.9 Reasonable Security Practices and Procedures

They shall secure all personal data that they have processed by reasonable security practices and procedures as specified under paragraph 27.1 of this Policy.

27. Transparency and accountability measures

27.1 Reasonable Security Practices and Procedures

(a) The data fiduciaries will implement such security practices and standards and have a comprehensive documented information security programme and Information Security Policy that contain managerial, technical, operational and physical security control measures that are commensurate with the data/information assets being protected by them.

(b) In the event of a data/information security breach, the data fiduciary shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they

have implemented security control measures as per their documented information security programme and information security policies.

(c) The data fiduciaries will, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of harm that may result from such processing, implement necessary security safeguards including the use of de-identification and encryption methods, methods to protect the integrity of the personal data collected, and methods to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data. Every data fiduciary shall undertake a review of its security safeguards in a periodic manner and take appropriate measures accordingly.

(d) 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.

(e) Subject always to the provisions of applicable laws, the standard(s) in relation to security practices and procedures mentioned above may be certified or audited on a regular basis through an independent auditor, duly approved by the Central Government. This audit shall be carried out by an auditor at least once a year or as and when the data fiduciary undertakes a significant upgradation of its processes, computer resources or systems.

(f) 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.

27.2 Data management by data processors

(a) The data fiduciary may conduct appropriate due diligence covering data privacy and security prior to engaging with any data processor.

(b) The data fiduciary may not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

(c) The data fiduciary will require its data processors to execute confidentiality agreements and non-disclosure agreements covering data protection and privacy responsibilities. Such agreements will be reviewed, updated and renewed on a periodic basis. The data fiduciary may require that the confidentiality requirements under such agreements continue for a specified period of time even after the contractual period ends.

(d) Subject to applicable law, the agreements referred to in clause (c) shall be in consonance with this Policy. These agreements shall ensure that data processors adhere to the same level of data protection that is adhered to by the data fiduciary.

(e) The data fiduciary will require its data processors to limit their access only to the personal data necessary for the fulfilment of their employment/contractual duties based on “need-to-know” principle, as the case may be.

(f) The data processor, and any employee of the data fiduciary or the data processor, will only process personal data in accordance with the instructions of the data fiduciary and treat it confidential.

(g) The data processor may not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in the contract referred to in clause (b) above.

(h) The data fiduciary will ensure that training and awareness materials around data protection and privacy are developed for its employees and data processors. Role-based training for individuals or teams considering the nature of processing and their role shall be developed. Data privacy training and awareness programs shall be conducted 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.

27.3 Data Protection Impact Assessment

(a) The data fiduciary will carry out a data protection impact assessment before it undertakes any processing involving new technologies or any other processing which carries a risk of significant harm to data principals.

(b) A data protection impact assessment shall contain, *inter alia*, a detailed description of the proposed processing operation, the purpose of processing, nature of personal data being processed, assessment of the potential harm and measures for managing, minimising, mitigating or removing such risk of harm.

27.4 Maintenance of Records

(a) The data fiduciaries will maintain accurate and up-to-date records to document the important operations in the data lifecycle including collection, transfers, and erasure of personal data and sensitive personal data. These will cover the following:

(i) details of the ecosystem partners;
(ii) purposes of the processing;
(iii) description of the categories of data principals;
(iv) description of the categories of personal and sensitive personal data;
(v) categories of recipients to whom the personal data/sensitive personal data is disclosed/transferred including to data processors; and
(vi) geographies of recipients.

(b) In addition to the records referred to above, the data fiduciaries will also maintain accurate and up-to-date records of the periodic review of security safeguards conducted under paragraph 27.1, data protection impact assessments conducted under paragraph 27.3 and requests received under paragraph 14 above.

27.5 Audit

(a) The data fiduciaries should maintain a strict audit trail of all activities which have access to any personal data, at all times. This may be reviewed by an appropriate authority such as an auditor, the legal representative of the data principal, the data principal, data protection officer, court appointed/authorised person, as deemed necessary.

(b) The data fiduciaries should also conduct a periodic audit to verify that its data processors and employees process all personal data appropriately in compliance with the privacy notices, confidentiality agreements, this Policy and the Information Security Policy.

(c) If the data fiduciary decides to update any personal data in accordance with paragraph 14.2 above, then the original personal data and an audit trail of the change shall be made available to the data principal. However, the updated personal data with a new version number shall be considered active. The advisory standard for audit trail /log in health record system is ISO 27789:2013 Health informatics - Audit Trails for Electronic Health Records.

Chapter VI: Sharing of personal data and obligations of entities with whom personal data is shared

28. Sharing of personal data by data fiduciaries

28.1 Any personal data processed by a data fiduciary may be shared with an HIU in response to a request made by such HIU for personal data pertaining to the data principal, only where consent of the data principal is obtained in accordance with Chapter III of this Policy.

28.2 Where an HIU makes a request for accessing any personal data under paragraph 28.1 above, the data fiduciary shall verify the consent shared with it, including whether such consent has been revoked by the data principal, and where the consent is valid, it shall share such data with the HIU strictly in accordance with Chapter III of this Policy.

28.3 A data fiduciary shall maintain a record of all consent obtained under this Policy, pursuant to which personal data has been shared by such fiduciary under this Policy in a manner that enables the audit and review of such data sharing.

28.4 Where the data principal has provided his/her consent for the sharing of their personal data under this Policy, it shall not be used, disclosed or shared by the data fiduciary or any HIU in any other manner or for any other purpose, except as provided in Chapter III of this Policy.

29. Sharing of de-identified or anonymised data by data fiduciaries

29.1 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.

29.2 The NHA shall set out a procedure through which any entity seeking access to anonymised or de-identified data under this Policy will be required to provide relevant information such as its name, purpose of use and nodal person of contact and, subject to approval being granted under this procedure, the anonymised or de-identified data under this Policy shall be made available to such entity on such terms as may be stipulated in this behalf.

29.3 Any entity which is provided access to de-identified or anonymised data shall not, knowingly or unknowingly, take any action which has the effect of re-identifying any data principal or of such data no longer remaining anonymised.

29.4 The de-identification or anonymisation of data by a data fiduciary shall be done in accordance with technical processes and anonymisation protocols which may be specified by the NHA in consultation with the MeitY.

29.5 The technical processes and anonymisation protocols referred to in paragraph 29.4 shall be periodically reviewed by the NHA and such review shall have regard to the nature and sensitivity of the data being processed, the risks of re-identification of data principals and the robustness of the anonymisation protocols.

30. Obligations of HIUs upon sharing of personal data

30.1 In addition to the obligations set out in Chapter V, a HIU shall ensure that any personal data under this Policy:

(a) shall not be used by the HIU for any purpose other than what was specified to the data principal at the time of obtaining his/her consent under Chapter III of this Policy;

(b) shall not be disclosed further without obtaining the consent of the data principal for such disclosure in the manner as specified in Chapter III of this Policy; and

(c) shall be provided the same level of data protection as a data fiduciary under this Policy and only be processed in accordance with this Policy, specifically provisions under Chapter V of this Policy

(d) shall not be retained beyond the period necessary for the purpose specified while obtaining consent under Chapter III of this Policy.

30.2 A HIU shall follow the principle of data minimisation and shall obtain the consent of the data principal only for such personal data that is necessary for the purposes for which such consent is being sought.

30.3 A HIU shall take all reasonable steps, including providing the data principal with a copy of the personal data received by such HIU from a data fiduciary to ensure that the data principal can exercise the rights as mentioned in paragraph 14 of this Policy.

30.4 A HIU shall, to the extent reasonable, maintain:

(a) a record of all personal data that is disclosed to any other entity, including the names of such entities, the time at which such personal data was disclosed and the categories of personal data which was disclosed; and

(b) a record of how such personal data is used by the HIU in a manner which enables the audit and review of any use of such personal data.

30.5 Any entity with whom an HIU has shared personal data, after obtaining the consent of the data principal as under paragraph 30.1 above, shall be subject to the same obligations as the HIU under this Policy and shall only process such personal data in strict accordance with the terms of the consent which authorises such sharing of personal data.

31. Restrictions on sharing, circulating or publishing of personal or sensitive personal data

31.1 Any personal data or sensitive personal data of the data principal shall not be published, displayed or posted publicly by any person or entity.

31.2 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.

Chapter VII: Grievance Redressal and Compliance

32. Grievance redressal

32.1 Data principals with inquiries and questions about the processing of their personal data may approach a designated officer of the data fiduciary (referred to as data protection officer) in writing, through email or any other electronic means, as may be specified. The details of the data protection officer shall be provided on the website of the data fiduciary along with the format and process for filing the inquiries/questions. It is clarified that where feasible, the data fiduciary may designate the data protection officer as the Grievance Officer mentioned in paragraph 32.2 below.

32.2 A complaint can be made by the data principal regarding any contravention of this Policy which has caused or is likely to cause harm to such data principal. The data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner. For this, the data fiduciary shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances of the data principal expeditiously but within one month from the date of receipt of grievance.

32.3 In the event that a complaint is not resolved by the Grievance Officer of the data fiduciary as referred to under paragraph 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 (_____). The details of the NDHM-DPO shall be displayed on the website (_____) along with the contact details and the format and processes for filing the above.

32.4 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.

32.5 Separately, in addition to the above, NHA shall maintain procedures for addressing and responding to all inquiries from data principals about the processing of personal data. NHA shall adequately publicise the existence of these procedures.

33. Personal Data Breach and Incident Management

33.1 The data fiduciary shall formulate and implement a personal data breach management mechanism, as may be stipulated and publicly displayed, which shall ensure that any instance of non-compliance with the provisions of this Policy, or any instance of unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data to a data principal is promptly reported to the incident response team of the NHA and other relevant entities.

33.2 NHA shall ensure that any instance referred to in paragraph 33.1 shall be notified to the relevant ecosystem entities and data principals within such time period as may be specified by the NHA

33.3 The NHA shall formulate and implement procedures to identify, track, review and investigate incidents referred to in paragraph 33.1, and shall maintain a record of such instances and actions taken pursuant to such instances.

33.4 The NHA shall provide notification of cyber security incidents to Cert-In as may be required under the provisions of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, in addition to any other notifications that may be required by applicable law.

33.5 Without prejudice to the foregoing, in the event of any incident of data breach, the person responsible for such breach shall be liable in accordance with the provisions of applicable law.

34. Compliance and Policy Governance

34.1 The NDHM-DPO shall ensure adherence to this Policy and shall be responsible for compliance with all applicable laws in force in India.

34.2 All individuals and entities who are covered by this Policy must comply with its requirements, and where requested demonstrate such compliance.

34.3 This Policy shall be revised at least once every year. A copy of this policy together with any significant revisions shall be made publicly available on the NDHM website (_____).

35. Non-compliance with this Policy

35.1 Where any entity/individual to which/whom this Policy is applicable is found to be in violation of any of its provisions, then an ID issued to such entity/individual under Chapter IV of this Policy, may be suspended or cancelled, and during such time of suspension or cancellation, such entity/individual shall not be permitted to participate in the NDHE. The procedures involved in such suspension/ cancellation and the details of the consequences thereof may be further set out by the NHA.

35.2 In addition, any failure to comply with this Policy may also result in action, such as, termination of service of employees or dismissal of interns/ volunteers of such entities, or termination of contracts or arrangements with any data processor/service provider entered into by such entities.

35.3 It is clarified that the above actions under this paragraph shall be without prejudice to any action that can be initiated under the provision of applicable laws.