सत्यमेव जयते national health authority

सत्यमेव जयते Ministry of Health and Family Welfare
Government of India

Ayushman Bharat Digital Mission

Draft Health Data Management Policy
April 2022, Version 02

Table of Contents

Glossary

Abbreviation	Expansion
ABDM	Ayushman Bharat Digital Mission
ABHA	Ayushman Bharat Health Account
CISO	Chief Information Security Officer
DPO	Data Protection Officer
EHR	Electronic Health Records
EMR	Electronic Medical Records
GRO	Grievance Redressal Officer
HFR	Health Facility Registry
HIE-CM	Health Information Exchange – Consent Manager
HIP	Health Information Provider
HIU	Health Information User
HPR	Healthcare Professionals Registry
MeitY	Ministry of Electronics and Information Technology
MoHFW	Ministry of Health and Family Welfare
NDHE	National Digital Health Ecosystem
NHA	National Health Authority
PHR	Personal Health Records
UTs	Union Territories of India

I: Preliminary

1. Purpose

The Ministry of Health and Family Welfare ("MoHFW") is responsible for conceiving the idea of the Ayushman Bharat Digital Mission ("ABDM"). 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 & 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 ("Blueprint") recommends that a federated architecture be adopted, instead of a centralised architecture, for the management of digital health data to ensure interoperability, technological flexibility and independence across the National Digital Health Ecosystem ("NDHE").

This Health Data Management Policy ("Policy") is the first step in realising the ABDM's guiding principle of "Security and Privacy by Design" for the protection of individuals'/data principal's personal digital health 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 will be dynamic in nature and may be revised from time to time as may be required. Necessary guidelines may also be issued for the implementation of the ABDM.

The NDHE is based on the principle of federated architecture, which allows interoperability between independent and decentralized information systems, while enhancing the security and privacy of personal data of individuals. Such interoperability shall be strictly compliant with the provisions relating to consent, and protection of personal data as set out under this Policy. This would be essential to build a trust quotient across the NDHE as well as to ensure that the personal data relating to the health of all individuals in India is adequately protected.

Currently, healthcare programs and facilities register patients/beneficiaries by numbers on their own leading to multiplicity of numbers. Therefore, numerous numbers are assigned to one individual across different healthcare facilities and programs. For creating an integrated, uniform and interoperable ecosystem in a patient or individual centric manner, all the government healthcare facilities and programs, in a gradual/phased manner, should start assigning the same number for providing any benefit to individual. This number, created with KYC using Aadhaar or any other digital system, will be known as Ayushman Bharat Health Account (ABHA(number)).

In addition, participation of an individual in the NDHE will be on a voluntary basis. Individual may link his/her health records with ABHA if he/she choose to do so. Linked health records can be shared after consent through Health Information Exchange - Consent Manager ("HIE-CM").

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, policies relating to information security, guidelines relating to data retention and archival, or any other policies or guidelines which may be notified from time to time for the implementation of the ABDM.

2. Applicability

The provisions of this Policy shall be applicable to all the entities and individuals who are part of the ABDM ecosystem. Illustrative list is as follows;

a) All individuals who have been issued an ABHA (number) or ABHA address under this policy;

b) healthcare professionals, including but not limited to doctors or healthcare practitioners (including those practicing recognised Indian systems of medicine such as Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homoeopathy), 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 facility which collects, stores and transmits personal data in electronic form in connection with its transactions;

f) payers such as Central Government, State Governments, insurers, health plans and charitable institutions;

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

h) research bodies such as institutions, individual researchers including researchers utilising data for health data analytics, statisticians, analysts and public health institutions;

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

j) 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 data within the ambit of the NDHE, including the Personal Health Identifier, the electronic health records and electronic medical records, by implementing adequate technical and organisational measures across the NDHE;

c) to create a system of digital health records which is easily accessible to individuals and healthcare service providers and is voluntary in nature, based on the consent of individuals, and in compliance with relevant standards;

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

e) to ensure 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) "ABHA" (number) or "Ayushman Bharat Health Account" (number) refers to the 14-digit Identification number allocated to a data principal in accordance with Chapter IV of this Policy;

b) "ABHA Address" is an address in the format (username)@HIE-CM. An ABHA Address may be used to link and share health records;

c) "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;

d) "child" means a natural person/individual who has not completed eighteen years of age;

e) "consent" means the consent referred to in Clause 9 of this Policy;

f) "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;

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) "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;

l) "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 ABDM integrated users (such as healthcare professionals 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;

m) "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;

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

o) "harm" means, --

   a. bodily or mental injury;
   b. loss, distortion or theft of identity;
   c. financial loss or loss of property;
   d. loss of reputation or humiliation;
   e. loss of employment;
   f. any discriminatory treatment;
   g. any subjection to blackmail or extortion;
   h. any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
   i. 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
   j. any observation or surveillance that is not reasonably expected by the data principal;

p) “health facility” refers to health establishments across the country including hospitals, clinics, diagnostic laboratories, health and wellness centres, imaging centres, pharmacies and others as may be specified by NHA from time to time;

q) “Health Information Exchange & Consent Manager” or “HIE-CM” refers to digital system which facilitates exchange of health information and management of consent.

r) “Health Information Provider” or “HIPs” means hospitals, diagnostic centres, public health programs, or other such entities integrated with the HFR or other entities which act as information providers (by generating, storing and distributing health records) in the digital health ecosystem;

s) “Health Information Users” or “HIUs” are entities that are permitted to request access to the personal data of a data principal and can access the same with the consent of the data principal in accordance with this Policy;

t) “Healthcare Professional ID” refers to the unique ID allocated to each healthcare professional in accordance with Chapter IV of this Policy;

u) “HFR” refers to the Health Facility Registry referred to in Clause 24.1 of this Policy. It is a comprehensive repository of health facilities of the nation across different systems of medicine that are recognised in India;

v) “HPR” refers to the Healthcare Professionals Registry referred to in Clause 21.2 of this Policy. It is a comprehensive repository of all healthcare professionals involved in the delivery of healthcare services across both modern and traditional systems of medicine;

w) “nominee”, for the purposes of this Policy, refers to a natural person/individual who has attained majority upon completing eighteen years of age and is authorized to take decisions with respect to health data which otherwise a major data principal of sound mind could take;

x) “official identifier” means any number, code, or other identifier assigned to a data principal under a law made by Parliament or any State Legislature or which may be issued by the NHA or any other identifier specified by the NHA, for the purpose of verifying the identity of a data principal;

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 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 PHR App, allowing only the individual, or people authorized by the individual, to access the medical data;

bb) "Personal Health Record Applications" or "PHR Apps" are software service providers which offer front ends to individuals and enable functionalities such as creating ABHA address, discovery & linking health records from various HIPs, allowing individuals to view their records, offering long term storage of records, uploading their health records and sharing records on the ABDM network. Every PHR App works closely with HIE-CM;

cc) "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;

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 sensitive personal data as defined under Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and shall include official identifiers;

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.

II: Entities under the NDHE, Applicable Law and Governance Structure

5. Entities under the NDHE and Applicable Laws

5.1. The NHA shall specify the procedure for permitting different classes of entities such as data fiduciaries, data processors, Health Information Providers, Health Information Users and repositories to operate in the NDHE.

5.2. Such procedures shall provide, inter alia, for the eligibility criteria, integration process, obligations, and terms and conditions for the entities mentioned in Clause 5.1 above.

5.3. All entities to which this Policy is applicable 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.

5.4. All entities as mentioned in Clause 5.1 above must adhere to and comply with all other relevant guidelines and policies as may be issued by NHA from time to time.

6. Governance Structure

The governance structure for the NDHE shall be as specified by the NHA. In addition, the governance structure shall consist of such committees, authorities and officers at the national, state, health facility and other levels as will be necessary to implement the ABDM. It shall consist of a data protection officer ("**ABDM-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. In addition to the ABDM-DPO, the governance structure of the NDHE shall also consist of a grievance redressal officer ("**ABDM-GRO**") who shall be responsible for carrying out the functions set out in Clause 32.3 of this Policy. It is further envisaged that the MoHFW and the Ministry of Electronics and Information Technology ("**MeitY**") shall provide overall guidance to the NHA on relevant aspects of the NDHE. Further specific details in relation to governance structure may be stipulated from time to time.

III: Consent Framework

7. Collection of Personal Data by Data Fiduciaries

Data fiduciaries can collect personal data, which shall be limited to such data that is necessary for the purposes specified under Clause 9.3 of 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 data by data fiduciaries:

a) Data principals should at all times have control and decision-making power over the manner in which 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 relevant national and international standards.

c) So far as sharing or disclosure of any 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 Data

9.1. Data fiduciaries can collect or process 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 Clause 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. The purposes for collection or processing of personal data shall be limited to those which may be specified by the NHA and such purposes will be related to the health of an individual or may be such other incidental purposes which a data principal can reasonably expect, having regard to the purpose and the context and circumstances in which the personal data was collected or processed.

9.4. In addition to the conditions mentioned in Clause 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 or Processing of 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 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 data of the data principal for any new or previously unidentified purpose.

10.2. It is clarified that for the purpose of Clauses 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.

The privacy notice should contain the following information:

a) the purposes for which the personal data is to be processed;

b) the nature and categories of personal data being collected by data fiduciary;

c) the methods or mechanisms by which the personal data is collected by the data fiduciaries;

d) the identity and contact details of the data fiduciary collecting the 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 data may be shared, if applicable;

g) the period of time for which the 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 Clause 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 data.

10.3. 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 Clauses 8 and 9 of this Policy, for collection, or further processing of personal data, may be obtained electronically or physically on paper, either directly from the data principal or through an HIE-CM, as the case may be. Where the consent is received physically on paper, then such consent may be converted to electronic form by the HIE-CM or the data fiduciary.

11.2. Where consent is obtained through an HIE-CM as set out above then such HIE-CM shall:

a) not access, process or store, in any manner whatsoever, the personal data shared with any data fiduciary pursuant to any consent obtained through such HIE-CM;

b) maintain a record of all consent shared and revoked, as the case may be, and

c) maintain a record of consent logs/consent transactions in a manner which enables the audit and review of any use of such data

11.3. Where the data principal has revoked his/her consent, it shall be the duty of the HIE-CM to notify the data fiduciary of such revocation, as applicable.

11.4. 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 HIE-CM or the data fiduciary to collect the personal data, or further process the personal data that has already been collected from the data principal for a particular purpose, as the case may be.

11.5. So far as further processing of personal data pursuant to Clauses 11.1, 11.3 and 11.4 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. The consent artifact will then be shared between the data principal and the Health Information Provider or a Health Information User, through an HIE-CM.

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

12. Processing Personal Data Pertaining to a Child

12.1. Data fiduciaries should ensure that the processing of the 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 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 data of the child as set out in Clause 12.2 above.

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

13. Processing personal data of data principals who are seriously ill or mentally incapacitated, or in response to a medical emergency involving a threat to the life or a severe threat to the health of the data principal

13.1. At the time a data principal opts to participate in the NDHE framework, such data principal should name a nominee.

13.2. The nominee referred to in Clause 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, or where the data principal is facing a threat to life or a severe threat to health and is unable to give valid consent.

13.3. In the event that the data principal has not named a nominee under Clause 13.1 above or nominee himself is also not able to give consent for any reason, 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 Clause 13.3 above only where there is proof of relationship with the data principal.

13.5. The personal data of a data principal can be processed without consent in the following exceptional situations –

a) Medical emergency where there is a threat to the life or health of the data principal; or

b) Interest of Public health; or

c) Order of the competent court.

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. a confirmation as to whether it has processed any personal data of the data principal;

B. the personal data that has been processed or a summary of the same;

C. summary of processing activities carried out on such personal data; and

D. any information provided under the notice issued in accordance with Clause 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) Restrict or object to disclosure: Subject to applicable law, the data principal can restrict or object to the disclosure of his/her personal data by the data fiduciary.

c) Data portability: As may be applicable, the data principal can request from the data fiduciary, a copy of the following in a structured, commonly used and machine-readable format, to the extent technically feasible or where compliance with such request would not reveal a trade secret:

i. the personal data provided to the data fiduciary; or

ii. the personal data which has been generated in the course of provision of services by the data fiduciary.

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

d) Exercising of any other right(s) as prescribed under applicable laws of the land.

14.2. General conditions for submitting requests

a) All requests under Clause 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 an HIE-CM.

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 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, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them. The data fiduciary will also notify the data principal once their request is accepted.

d) In the event that any request 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 nominee of the data principal may have access to the personal data of the data principal, only if such access by such person was specifically 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 Clause 14.1 above.

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

IV: ABHA & Other ID Policy

15. Allocation of ABHA (number)

15.1 ABHA (number) may be created at no cost. During the process, the data principal will be required to establish his/her unique identity.

15.2 An ABHA (number) may be issued through such means as may be specified by the NHA.

15.3 An ABHA (number) remains the primary source of demographic details of the data principal in NDHE.

15.4 A data principal shall have only one ABHA (number), which shall be linked to his /her Aadhaar or any other KYC document such as PAN, Driving License, Passport and others as may be specified by the NHA from time to time.

15.5 An ABHA (number) may be verified by using a data principal’s Aadhaar number or any other method of identification as may be specified by the NHA from time to time.

15.6 A data principal may link his/her one or more than one ABHA Addresses to his/her ABHA (number), and shall retain control over the linking or de-linking of their ABHA Addresses with their ABHA (number).

16. Creation of ABHA (number)

16.1 The IT platforms which are integrated to ABDM (through sandbox environment) can be utilized for creating ABHA number for individuals.

16.2 ABHA (number) shall be issued to data principal visiting government healthcare institutions or participating in government healthcare programs for availing healthcare services. This will be applicable across all government healthcare institutions and programs. The data principal may voluntarily use the same ABHA (number) with other healthcare institutions also.

16.3 At the time of creation of ABHA (number), data principal shall declare that he/she has not been issued ABHA (number) in past. For creation of ABHA (number) through IT platforms referred in Clause 16.1, it shall be the responsibility of the IT platforms to obtain such declaration from the data principal.

17 Allocation of ABHA Address

17.1 A data principal may take services of ABDM or an integrated HIE-CM in the NDHE or through such means as may be specified by NHA for creation of an ABHA Address.

17.2 The personal data of data principal may be linked to his/her ABHA Address if consent for such linking is provided by him/her for the purpose of creating longitudinal health record.

17.3 A clear log of the consent given by a data principal shall be maintained and every such instance of consent given by a data principal shall be accessible to the data principal through his/her ABHA Address.

17.4 A data principal shall be able to provide or revoke his/her consent in order to enable or restrict any sharing of personal data linked with his/her ABHA Address, and shall be able to update his/her personal data in accordance with this Policy.

18 Creation of ABHA Address

18.1 An HIE-CM wishing to issue a ABHA Address can integrate with the ABDM. The integration process and functioning of such HIE-CM shall be as per the guidelines as prescribed by NHA from time to time.

18.2 There shall exist multiple HIE-CM in the NDHE.A data principal may select any HIE-CM of his/her choice for creation of ABHA Address. The data principal may hold multiple ABHA Addresses at a time.

18.3 For the data principals visiting government healthcare facilities or participating in government healthcare programs, a default ABHA Address shall be created along with the ABHA (number) as referred in Clause 16.2 for enabling the linking, collecting and sharing of personal data by the data principal. The default ABHA Address would look like (ABHAnumber)@HIE-CM. Additionally, data principal may also create another ABHA Address of his/her choice which would look like (userchosen)@HIE-CM.

19 Principle of Non-exclusion for Data Principal

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

19.2 The NHA shall ensure that the means of verification that are specified under Clause 15.5 of this Policy do not have the effect of preventing an individual not in possession of an Aadhaar number from being issued an ABHA (number).

19.3 No individual shall be denied access to any health facility or service or any other right in any manner by any government or private entity, merely by reason of not creating a ABHA Address or ABHA (number) or disclosing his/her ABHA (number), or denying consent for processing of personal data which is not necessary for providing health services, or for not being in possession of a ABHA Address or ABHA (number), or for not choosing to participate in the NDHE.

19.4 Pursuant to Clause 12 of this Policy, it is clarified that the parent or guardian of a child may request for the creation of a ABHA Address and ABHA (number) on behalf of such child in accordance with Chapter III of this Policy and applicable law.

20 Allocation of a Healthcare Professional ID

20.1. The processing of personal data for the creation of a Healthcare Professional ID must be in accordance with the data protection principles set out in this Policy.

20.2. A healthcare professional may request for the creation of a Healthcare Professional ID at no cost, which will be required to enable them to participate in the NDHE as set out under this Policy.

20.3. A Healthcare Professional ID may be issued through such means as may be specified by the NHA.

20.4. A Healthcare Professional ID shall be in electronic form, and a healthcare professional in possession of a Healthcare Professional ID shall not be permitted to create a second ID. Such Healthcare Professional ID shall be non-transferrable.

20.5. A healthcare professional may electronically sign documents, such as e-prescriptions, diagnostic reports, discharge summaries and e-claims using his/her Healthcare Professional ID.

20.6. A Healthcare Professional ID may be used to authenticate/verify a healthcare professional digitally for services created by the ABDM as part of the NDHE, including tele-medicine and other healthcare services.

21 Creation of Healthcare Professional ID

21.1. A healthcare professional may be required to verify his/her professional credentials, and any updates to such credentials, through the respective council, board, department, regulatory or professional body which governs their practice or through any other agency as may be notified by NHA in order to create a valid Healthcare Professional ID.

21.2 Upon verification of the professional credentials by the NHA through the concerned authorities as under Clause 21.1 or their work details by the Central Government /State Government/UT administration, such healthcare professionals may be issued a Healthcare Professional ID and included in the HPR.

22 Principle of Non-exclusion for Healthcare Professional ID

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

22.2. It is clarified that the right of a qualified healthcare professional 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 Healthcare Professional ID or for not choosing to participate in the NDHE.

23 Allocation of Facility ID

23.1. A health facility in India may request for the creation of a Facility ID at no cost, which shall be required to enable them to participate in the NDHE as set out under this Policy.

23.2. A Facility ID may be issued through such means as may be specified by the NHA.

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

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

23.5. The Facility ID may be used to electronically sign all documents, which are necessary to provide healthcare services.

23.6. The possession of a 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.

24 Creation of Facility ID

24.1. A health facility may register their facility for a Facility ID as per the registration procedure as may be specified by the NHA. A health facility possessing a Facility ID shall be included as part of the HFR.

24.2. The NHA shall put in a mechanism to update the status of health facilities so as to ensure that correct details about the health facilities are available through the registry. The procedure for verification of health facilities may be notified by NHA from time to time.

24.3. The owner or manager of a health facility may update details of such facility through the web portal / mobile application, or any other mode as may be specified by the NHA.

25 Principle of Non-exclusion for Facility ID

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

25.2. 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 Facility ID or for not choosing to participate in the NDHE.

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 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 to the NHA as may be required:

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 that no personal data other than what is required at a minimum to create and maintain ABHA (numbers), Facility IDs or Health Professional IDs shall be stored centrally. Electronic medical records shall be stored at the health facility where such records are created, or at such other entities as may be specified under Clause 5 of this Policy. Electronic health records shall be maintained by entities specified under Clause 5 of this Policy, as a collection of links to the related medical records. The NHA shall issue appropriate technological and operational guidelines for ensuring the security & privacy of the personal data of data principals, and for maintenance of electronic medical records & electronic health records.

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, the data fiduciary 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.

The privacy policy issued and the principles of privacy by design followed by the data fiduciaries should be in consonance with this Policy and applicable law.

26.4. Choice and Consent Driven Sharing

They will take consent from data principals in accordance with Clause 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 Clause 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 Clause 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. 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 Clause 14 of this Policy as well as any guidelines relating to data retention and archival that may be notified from time to time. The data fiduciary will undertake a periodic review to determine whether it is necessary to retain the personal data in its possession. No personal data shall be stored beyond the geographical boundaries of India, subject always to the provision of applicable laws.

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 per Clause 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 erased or amended without following the due process referred to in Clause 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 Clause 27.1 of this Policy.

27 Transparency and Accountability Measures

27.1. Reasonable Security Practices and Procedures

a) The data fiduciaries will implement reasonable 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 any 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 deidentification 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) 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.

e) In the case of any entities who are implementing/involved in the ABDM and acting as a data fiduciary in this regard, the Chief Information Security Officer ("ABDM-CISO") and the ABDM-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 nondisclosure 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. 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; and

   v. categories of recipients to whom the personal data is disclosed/transferred including to data processors.

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

27.5. Audit

a) The data fiduciaries should maintain a strict audit trail of all processing activities which have access to any personal data, at all times. A record of how such personal data is processed by the data fiduciary should also be maintained in a manner that enables the audit and review of any use of such personal data.

b) Data fiduciaries should ensure that periodic audits of its data processors are conducted by third parties in accordance with relevant standards and certifications, as may be specified by the NHA, to verify that such data processors process all personal data appropriately in compliance with the privacy notices, contracts/confidentiality agreements, this Policy and any policy relating to information security as may be notified from time to time.

c) If the data fiduciary decides to update any personal data in accordance with Clause 14.2 of this Policy, 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.

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 Clause 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 the 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 as per the procedure set out in Clause 29.5 below 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 deidentified 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 permission 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 data fiduciary which is undertaking to anonymise or de-identify data under this Policy shall be responsible for ensuring compliance with the procedure for such anonymisation or de-identification as set out by the NHA in Clause 29.5 and any non-compliance will be dealt with as per Clause 35.

29.5. 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.

29.6. The technical processes and anonymisation protocols referred to in Clause 29.5 above 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, an 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. An 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. An 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 Clause 14 of this Policy.

30.4. An HIU shall 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) to the extent reasonable, 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 under Clause 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 Data

31.1. Any 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 Clauses 29.2 and 29.5 of this Policy.

VII: Grievance Redressal and Compliance

32 Grievance Redressal

32.1. A data principal with inquiries and questions about the processing of his/her 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 Clause 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 Clause 32.2 above, the matter may be referred to the ABDM-GRO in writing or through an email ID or any other electronic means provided under the grievance portal of ABDM website. The details of the ABDM-GRO shall be displayed on the website along with the procedure for contact and the format and processes for filing the above.

33 Personal Data Breach and Incident Management

33.1. The data fiduciary shall formulate and implement a personal data breach management procedure, which will be publicly displayed. The data fiduciary will also 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 notified to relevant entities as may be required by applicable law, including the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

33.2. The data fiduciary shall notify any incidents referred to in Clause 33.1 and the actions taken pursuant to such incidents, to the data principal and NHA as soon as possible and within such period as may be specified by NHA from time to time, as well as any applicable law.

33.3. Without prejudice to the foregoing, in the event of any incident of personal 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 ABDM-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 may be revised from time to time. A copy of this policy together with any significant revisions shall be made publicly available on the ABDM website.

35 Non-compliance with this Policy

35.1. Where any person to whom this Policy is applicable is found to be in violation of any of its provisions, such person may not be permitted to participate in the NDHE. Additionally, any Facility ID or Healthcare Professional ID issued to any person under Chapter IV of this Policy, may be suspended or cancelled. The detailed procedures involved in relation to any suspension or cancellation as mentioned above shall be set out by the NHA.

Explanation: For the purpose of this clause, “person” includes any data fiduciary, data processor, entity responsible for managing HIE-CM, Health Information Provider, Health Information User, health facility and healthcare professional.”

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