Ministry of Health and Family Welfare
Government of India

national health authority

National Digital Health Mission

DATA PRIVACY POLICY

1. Background of the National Digital Health Mission

The Ministry of Health and Family Welfare ("MoHFW") conceptualised the National Digital Health Mission ("NDHM"). It also created the National Digital Health Blueprint, 2019 (the "Blueprint"), which sets out the building blocks and action plan to comprehensively and holistically implement a national digital health ecosystem ("NDHE") which supports universal health coverage in an efficient, accessible, inclusive, timely and safe manner. The NDHM was envisaged as a mission to carry out the implementation of the Blueprint in order to create a digital ecosystem for healthcare services in the country. The NDHM Health Data Management Policy is a step in realising the NDHM's guiding principle of "Security and Privacy by Design" for the protection of individuals' personal digital health privacy. It acts as a guidance document across the NDHE and sets out the minimum standards for data privacy protection that should be followed to ensure compliance with relevant and applicable law, rules and regulations.

2. Purpose of the NDHM Privacy Policy

The NDHM is committed to the protection of privacy of data and will take all reasonable steps to protect the personal data belonging to participants in the NDHM ecosystem. Participation of an individual in the NDHE will be on a purely voluntary basis.

This document (or the "NDHM Privacy Policy") has been prepared pursuant to the requirement set out under Clause 26.3 of the NDHM Health Data Management Policy and it outlines the manner in which the NDHM and its ecosystem partners collect, process and use personal data of individuals. The NDHM Privacy Policy sets out the minimum standard of data protection and information security principles and is intended to act as a guide to the NDHM and its ecosystem partners in the process of collection, use and processing of personal data.

The NDHM Privacy 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, the NDHM Health Data Management Policy, or any other policies or guidelines, which may be notified by the Central Government from time to time for the implementation of the NDHM.

3. Applicability

The provisions of the NDHM Privacy Policy shall be applicable to the entities involved in the NDHM and the partners/persons/processes who or which are a part of the NDHE, and who/which are involved in the collection, use or any other form of processing of personal data and sensitive personal data. This is also reflected in Clause 2 of the NDHM Health Data Management Policy.

4. Mechanisms for Collection of Personal Data

Data fiduciaries may collect personal and sensitive data in accordance with Clause 7 of the NDHM Health Data Management Policy for the purposes set out in Clause 9 of the NDHM Health Data Management Policy and those specified by the NDHM by way of notifications that may be issued from time to time in this regard.

5. Privacy Principles

The NDHM adopts the following nine principles to govern the use, collection, and processing of personal and sensitive personal data:

Principle 1: Accountability

Pursuant to Clause 26.1 of the NDHM Health Data Management Policy, the NDHM and its ecosystem partners as data fiduciaries shall be accountable for complying with measures which give effect to the privacy principles while processing any personal data by it or on its behalf. In addition, 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 as per Clause 8(a) of the NDHM Health Data Management Policy.

Principle 2: Transparency

Pursuant to Clause 26.2 of the NDHM Health Data Management Policy, NDHM and its ecosystem partners as data fiduciaries shall make readily available to its employees, data principals and ecosystem partners specific information about its policies and practices relating to the management of personal data. This information may include categories of personal data collected, the purposes for which it is collected, collection of personal data that is likely to cause significant harm, the rights of the data principal in relation to their personal data, grievance redressal procedures, and data trust scores of the data fiduciary where applicable. In addition to the information specified above, the NDHM and its ecosystem partners as data fiduciaries will 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. All necessary steps shall be taken to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the personal data they collect, in order to ensure compliance with the privacy principles.

Principle 3: Choice & Consent

The knowledge and consent of a data principal are required for the collection, use or disclosure of personal data. As per the NDHM Health Data Management Policy, the NDHM and its ecosystem partners shall provide an option to data principal to opt-in/opt-out of the NDHE at any time or choose not to provide the information sought at any given time.

1. **Choice**

The consent given by the data principal must be free, informed, clear and specific with respect to the purpose identified in the privacy notice issued under Clause 10 of the NDHM Health Data

Management Policy. The consent form that is provided to the data principal by the data fiduciary must mention that consent is voluntary, and that refusal to provide consent/ revoke consent at any time will attract no penalty or loss of benefits to which the data principal is otherwise entitled by the Central and respective state Government and any healthcare providers.

2. **Consent**

The consent form must enable the data principal to make an informed decision regarding data for which he/she intends to give consent, purpose of usage of data clearly and unambiguously and the duration for which data may be retained. As per Clause 10.2 of the NDHM Health Data Management Policy, a fresh consent will be taken in case there is any change in privacy policy, or procedure, or a new purpose is identified other than the one(s) previously identified.

(a) **Means of obtaining Consent:** As per Clause 11.1 of the NDHM Health Data Management Policy, the consent of the data principal may be obtained through NDHM/ ecosystem partners' website or mobile application electronically or physically on paper directly or through a consent manager*("consent manager" means an electronic system that interacts with the data principal and obtains consent from him/her for any intended access to personal data)*. 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.

(b) **Types of Consent**: As stipulated in Clause 9.1 of the NDHM Health Data Management Policy, the data fiduciary must obtain valid consent of the data principal for the collection and processing of personal data. Consent may be obtained directly from the data principal or may be given by a nominee as set out under the NDHM Health Data Management Policy. Consent may be given by a person other than the data principal in the following circumstances:

(i) **Consent provided on behalf of a child**: Clause 12 of the NDHM Health Data Management Policy states that the parent or legal guardian can give consent on behalf of a child below the age of 18 years.

(ii) **Serious illness or mental incapacitation:** Clause 13 of the NDHM Health Data Management Policy sets out that the nominee of the data principal is authorised to give valid consent on behalf of a data principal who is seriously ill or mentally incapacitated or who is facing a severe threat to life or health and is unable to give valid consent. Where the data principal has not declared a nominee to act on his or her behalf, then any adult family member of the data principal may provide valid consent on behalf of the data principal only when there is proof of relationship with the data principal.

(iii) **Death of Data Principal**: Clause 14.2(e) of the NDHM Health Data Management Policy stipulates that in the event of the death of a data principal, then the nominee of the data principal may have access to the personal data of the data principal if such access by such person was specifically consented to by the data principal.

3. Please note that personal data may be collected, used or disclosed only with the consent of the nominee, parent, or guardian of the data principal, who has been authorised to provide valid consent on behalf of the data principal.

4. The data fiduciary must comply with the policies or guidelines in relation to consent that may be notified by the NDHM from time to time.

5. Any retention or storage of Aadhaar number or any other document used for identification must be in accordance with applicable law.

6. As per Clause 10.4 of the NDHM Health Data Management Policy, the privacy notice that is provided to a data principal shall be clear, concise and easily comprehensible to a reasonable person.

7. **Principle 4: Privacy by Design**

1. As set out under Clause 26.3 of the NDHM Health Data Management Policy, the NDHM and its ecosystem partners as data fiduciaries shall consider data protection requirements as part of the design and implementation of systems, services, products and business practices.

2. Data fiduciaries must also make available a privacy by design policy on their websites containing information relating to:
   (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.

3. The principles of privacy by design followed by the data fiduciaries should be in consonance with the NDHM Health Data Management Policy and applicable law.

Principle 5: Collection, Use and Storage Limitation

As set out under Clause 26.6 of the NDHM Health Data Management Policy, the NDHM and its ecosystem partners as data fiduciaries shall ensure that:

(a) collection and use of personal data from data principals is done only to the extent necessary for the purposes of processing;
(b) the processing of all personal data will be in a fair and reasonable manner, ensuring the privacy of the data principal;
(c) No personal data shall be transferred by the data fiduciary unless such transfer is in accordance with the NDHM Health Data Management Policy and the privacy policy of the data fiduciary, subject always to the provisions of applicable laws;

(d) 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 the Policy as well as any guidelines for data retention and archival as may be notified from time to time;
(e) personal data may be retained for a longer period of time if explicitly specifically consented to by the data principal or if such retention is necessary to comply with any obligation under any applicable law; and
(f) the data fiduciary will undertake a periodic review to determine whether it is necessary to retain the personal data in its possession.

Principle 6: 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 the NDHM Health Data Management Policy and consented by the data principal. Further, the purposes for which personal data may be collected by data fiduciaries will be limited to those which may be specified by the NDHM under notifications which may be issued from time to time 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.

Principle 7: Empowerment and rights of the data principal

1. The NDHM and its ecosystem partners must believe in strengthening the rights of data principals in relation to their personal data.
2. The data principal has the rights provided to them under Clause 14 of the NDHM Health Data Management Policy, in addition to any rights under applicable law. These rights include:
   (a) the right to confirmation and access as under Clause 14.1(a) of the NDHM-Health Data Management Policy;
   (b) the right to correction and erasure as under Clause 14.1(b) of the NDHM Health Data Management Policy;
   (c) The right to restrict or object to disclosure as under Clause 14.1(c) of the NDHM Health Data Management Policy;
   (d) The right to data portability as under Clause 14.1(d) of the NDHM Health Data Management Policy;
   (e) the right to revoke their consent;
   (f) The right to lodge a complaint or grievance with the Data Protection Officer of the data fiduciary, or with the NDHM-Grievance Redressal Officer ("**NDHM-GRO**") as under Clause 32 of the NDHM Health Data Management Policy.

3. In the event that the data principal wishes to exercise these rights with respect to the data fiduciary, then he/she must do so in accordance with the procedure set out in the data fiduciary's privacy notice and the NDHM Health Data Management Policy. The data fiduciary will provide contact details in a clear and unambiguous manner. The details will include name of the contact person, address, phone number, email id of data fiduciary collecting data as well as the contact details of the individuals or entities such as other data fiduciaries or data processors with whom personal data may be shared.

4. In the event that the data principal has wishes to lodge a complaint with the NDHM-Data Protection Officer, then it may do so as set out below:

   Name of the NDHM-Data Protection Officer:
   Phone Number:
   Email ID:

5. The NDHM and its ecosystem partners shall not restrict any data principal requesting their data based on factors such as language, disability status, technological knowledge, etc.

6. The NDHM and its ecosystem partners shall oversee the fulfilling of such requests and provide a justification in writing in case of denial of such requests.

7. The NDHM and its ecosystem partners shall maintain records of such requests irrespective of their fulfilment status.

Principle 8: Minimum Necessary Uses & Disclosures

1. NDHM and its ecosystem partners shall make reasonable efforts to use, disclose, and request only the minimum amount of personal data needed to accomplish the intended purpose of the use, disclosure, or request.
2. NDHM as data fiduciary shall not disclose personal data to third parties, except after providing notice and seeking informed consent from the individual for such disclosure.

Principle 9: Security Safeguards

The NDHM and its ecosystem partners must adopt the principles in relation to security standards and accountability as set out under Clauses 27.1, 27.2, 27.3 27.4 and 27.5 of the NDHM Health Data Management Policy. This would include:

(a) data management protocols to be followed by data processors;
(b) data protection impact assessments that must be carried out before a data fiduciary undertakes any processing involving new technologies or any other processing which carries a risk of significant harm to data principals;
(c) maintenance of accurate and up-to-date records to document the important operations in the data lifecycle including collection, transfers, and erasure of personal data;
(d) maintenance of a strict audit trail of all processing activities which have access to any personal data, at all times; and
(e) maintenance of a record of how such personal data is processed by the data fiduciary in a manner that enables the audit and review of any use of such personal data.