# NHA Data Privacy Policy

## PRADHAN MANTRI JAN AROGYA YOJANA (PM-JAY)

**VERSION 3.0**

**June, 2023**

## Preface

**Ayushman Bharat,** a flagship scheme of Government of India was launched as recommended by the National Health Policy 2017, to achieve the vision of Universal Health Coverage (UHC). It aims to undertake path breaking interventions to holistically address health (covering prevention, promotion and ambulatory care), at primary, secondary and tertiary level. Ayushman Bharat adopts a continuum of care approach, comprising of two inter-related components, which are -

1. **Pradhan Mantri Jan Arogya Yojana (PM-JAY)**
2. **Health and Wellness Centres (HWCs)**

**Pradhan Mantri Jan Arogya Yojana (PM-JAY)** is a **Mega Health Insurance Scheme** that has the benefit cover of Rs. 5 lakh per family per year. It has aimed to provide health insurance/assurance coverage for over 10 crores poor and vulnerable families targeting around 50 Crores persons, for Rs.5 lakh per family on family floater basis in any empaneled hospital on cashless and paperless basis. **Health and Wellness Centres**, are envisaged to deliver an expanded range of services to address the primary health care needs of the entire population in their area, expanding access, universality and equity close to the community.

It is committed to ensure highest possible level of health and well-being for all, through a preventive

It is committed to ensure highest possible level of health and well-being for all, through a preventive and encouraging health care orientation in developmental policies and universal access to good quality health care services without anyone having to face financial hardship.

In order to facilitate the effective implementation of the scheme, the State Government shall set up the State Health Agency (SHA) or designate this function under any existing agency/ trust/ society designated for this purpose, such as the State nodal agency for RSBY or a trust/ society set up for a State insurance program. States will have the option to use an existing Trust/ Society/ Not for Profit Company or set up a new Trust/ Society/ Not for Profit Company [State Health Agency, SHA] to implement the scheme. With respect to implementation, the States will be free to choose the modalities for implementation. They can implement the scheme through insurance company or directly through the Trust/ Society or mixed model. The SHA shall be responsible for delivery of the services under PM-JAY at the State level.

In provision of the welfare of poor and vulnerable residents, as part of PM-JAY solution, NHA uses individual's personal identifiable information, to establish identity of the beneficiaries and provide scheme benefits, which entails collection and processing of health data of the beneficiaries. The entire ecosystem of PM-JAY uses, collects, process, transmits, stores and securely disposes the personal data at several stages. Consequently, NHA is committed to protect individual's personal data and health data through the implementation of appropriate controls for safeguarding privacy of such data.

This Data Privacy Policy document specifies how NHA handles personal data and health data of the beneficiaries as well as the personal data of its employees and ecosystem partners.

## Terms & Definitions

**"Arogya Mitras**" are facilitators to be placed in each hospital empanelled with PM-JAY to facilitate the enrolment, patient admission and claim process for the beneficiaries of the mission. They will also act as interface between the hospital and insurance company/ trust.

"**Anonymization**" is the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified.

**"Biometric Information"** 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 behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person.

**"Consent"** means expressed informed consent, whether in written or electronic form, given by the data owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of his/her personal data.

**"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.

**"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

**"Data Principal"** means the natural person to whom the personal data belongs.

**"De-identification"** is the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's personal data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.

**"Electronic Consent"** is the digital equivalent of a physical letter of permission given by the user which, when presented, allows the data provider to share data regarding the user with a data consumer, for a particular purpose. Just as Aadhaar e-KYC, e-Sign, and Digital Locker provide digital equivalents of the corresponding physical paper based process, electronic consent allows for data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability to ensure that the data trails can be audited in the future.

**"Electronic Data Interchange (EDI)"** is the concept of businesses electronically communicating information that was traditionally communicated on paper, such as purchase orders and invoices.

**"Electronic Medical Record (EMR)"** relating to an episode or a set of episodes relating to a patient, is maintained at the facility level. These are digital versions of the paper charts in clinician offices, clinics, and hospitals. EMRs contain notes and information collected by and for the clinicians in that office, clinic, or hospital and are mostly used by providers for diagnosis and treatment. EMRs are more valuable than paper records

because they enable providers to track data over time, identify patients for preventive visits and screenings, monitor patients, and improve health care quality.

**"Electronic Health Record (EHR)"** is a longitudinal record of a particular patient across several facilities and is maintained as a collection of links to the primary data (EMRs).These are built to go beyond standard clinical data collected in a provider's office and are inclusive of a broader view of a patient's care. EHRs contain information from all the clinicians involved in a patient's care and all authorized clinicians involved in a patient's care can access the information to provide care to that patient. EHRs also share information with other health care providers, such as laboratories and specialists, subject to the consent of the patient. EHRs follow patients – to the specialist, the hospital, the nursing home, or even across the country.

**"Health data"** means data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.

**"Personal data"** means any data or information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available or likely to be available with a body corporate, is capable of identifying such person.

**"Personally Identifiable Information (PII)"** is the data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

"Personal Health Record (PHR)" contain the same types of information as EHRs—diagnoses, medications, immunizations, family medical histories, and provider contact information—but are designed to be set up, accessed, and managed by patients. Patients can use PHRs to maintain and manage their health information in Health Locker. PHRs can include information from a variety of sources including clinicians, home monitoring devices, and patients themselves.

**"Personnel"** All officers, employees, staff and other individuals employed or engaged by NHA or by the service providers supporting PM-JAY ecosystem.

**"Processing"** Any operation performed on personal data, whether or not by automated means, including collection, use, recording, holding, accessing, etc.

"Profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behavior, attributes or interest of a data principal.

**"Pseudonymization"** It is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

"Re-identification" means the process by which a data fiduciary or data processor may reverse a process of de-identification;

**"Sensitive personal data"** means such personal data or information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit. Such personal data, consists of information relating but not limited to;

- Password
- Financial information such as bank account or credit card or debit card or other payment instrument details
- Physical, physiological and mental health conditions
- Sexual Orientation
- Medical records and history
- Biometric information

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as Sensitive Personal Information for these purposes.

**"Third Party"** Any entity in relation to personal data, means any person other than the data principal, the data Fiduciary, or any data processor or other person authorized to process data for the data Fiduciary.

**"Unique Health Id (UHID)"** is a unique identifier for each patient or beneficiaries' that serves as a key to a patient's or beneficiaries' health record. Further details on it can be referred in the National Digital Health Blueprint (NDHB) published by Ministry of Health and Family Welfare (MoHFW).

## 1. Introduction

**Ayushman Bharat,** a flagship scheme of Government of India was launched as recommended by the National Health Policy 2017, to achieve the vision of Universal Health Coverage (UHC). It aims to undertake path breaking interventions to holistically address health (covering prevention, promotion and ambulatory care), at primary, secondary and tertiary level. Ayushman Bharat adopts a continuum of care approach, comprising of two inter-related components, which are -

- **Pradhan Mantri Jan Arogya Yojana (PM-JAY)**
- **Health and Wellness Centres (HWCs)**

**Pradhan Mantri Jan Arogya Yojana** will cover over 10 crore poor and vulnerable families (approximately 50 crore beneficiaries) providing coverage up to 5 lakh rupees per family per year for secondary and tertiary care hospitalization. Benefits of the scheme are portable across the country and a beneficiary covered under the scheme will be allowed to take cashless benefits from any public/private empanelled hospitals across the country. **Health and Wellness Centres**, are envisaged to deliver an expanded range of services to address the primary health care needs of the entire population in their area, expanding access, universality and equity close to the community.

One of the core principles of Pradhan Mantri Jan Arogya Yojana is to adopt co-operative federalism and provide flexibility to states. For giving policy directions and fostering coordination between Centre and States, **Pradhan Mantri Jan Arogya Yojana Council** (PMJAYC) has been set up at the apex level and it is chaired by Union Health and Family Welfare Minister.

**National Health Authority** has been established at the national level to manage and coordinate matters relating to the mission. States/ UTs have advised to implement the scheme through a dedicated entity called **State Health Agency (SHA).** They can either use an existing Trust/ Society/ Not for Profit Company/ State Nodal Agency (SNA) or set up a new entity to implement the scheme. States/ UTs can decide to implement the scheme through an insurance company or directly through the Trust/ Society or use an integrated model.

In partnership with NITI Aayog, a robust, modular, scalable and interoperable IT platform has been established to ensure a paperless, cashless transaction. The platform will be shared with States after making appropriate customizations relevant to each state. States can add additional features and functionalities in a modular approach. Within SHA there would be a qualified team to manage this IT system. Those States having their own well-defined IT system need to share certain data fields on real time basis, such as balance check, national portability claims etc.

NHA is committed to maintain the accuracy, confidentiality, security and privacy of beneficiaries, in respect of personally & sensitive personal data.

## 2. Purpose

National Health Authority (NHA) is committed to the protection of beneficiaries' privacy and will take all reasonable steps to protect the personal data belonging to beneficiaries' or any individual who is a part of Pradhan Mantri Jan Arogya Yojana (PM-JAY).

This policy outlines how NHA and its eco system partners collect, process and use personal data of beneficiaries and other individuals in compliance with Aadhaar Act 2016, IT Act 2000 and Right to Information (RTI) Act and rules and regulations thereunder. This Policy sets out the minimum standard and shall guide all NHA employees and its eco system partners.

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable laws (mentioned above) and other binding agreements.

## 3. Applicability

This policy applies to all the employees of National Health Authority (NHA), State Health Agency (SHA), Service Providers, Hospitals, Insurers, Consultants, any PM-JAY ecosystem partner or any entity involved in the collection, use, disclosure, retention and storage of the PII and SPI of the beneficiaries or any individuals connected with the scheme.. The applicability of the policy is as follows:

a) All individuals, teams, entities or eco system partners who collect or process personal data of beneficiaries or any individuals as part of PM-JAY
b) All methods of contact, including in person, written, via the Internet, direct mail, telephone, or facsimile

## 4. Objective

The key objectives of this policy are:

a) To provide adequate guidance and framework for the secure handling of PII and SPI of the beneficiaries of the Scheme in compliance with all laws and regulations applicable to NHA.
b) Increase awareness of the pivotal importance of data privacy and instil a privacy-oriented mind-set among the members of NHA and its eco system partners
c) Safeguard personal data, including PII and SPI, by implementing adequate technical and organizational measures.
d) Establish appropriate institutional mechanisms for auditing of the eco-system as needed, to provide assurance of the compliance with this data privacy policy by all the stakeholders.

## 5. Mechanisms for Collection of Personal Data

The following mechanisms are adopted for collection of Personal & Sensitive Personal Data in the course of the implementation of the Scheme:

a) **Directly, where the data principal is aware:** Here the data principal is aware or cognizant of the data being collected. For e.g. when the data principal voluntarily provides the data or authorizes the NHA and its ecosystem partners to collect the data on his/her behalf from a third party.
b) **Directly, where the data principal may not be aware:** Here the data principal may not be aware or cognizant of the personal data being collected. For e.g. information collected (website cookies etc.) by the NHA and its ecosystem partners when the data principal is using the services of the NHA and its ecosystem partners online or via the other sources
c) **Indirectly, where the data principal may not be aware:** Here the data may be collected from third party sources or databases about the data principal without the data principal being aware of such collection.

NHA and its ecosystem partners may collect data from various sources like SECC, RSBY, and State Databases for beneficiary's enrolment to PM-JAY system.

## 6. Type of Personal & Sensitive Personal Data Collected

The personal data collected by NHA and its ecosystem partners for PM-JAY includes the following:

**a) Beneficiaries Identity Information required for enrolment to the Scheme**

- Name
- Name of relative (i.e. s/o, d/o, w/o)
- Date of Birth
- Gender
- Residential Address
- Mobile Number
- Email Address

**b) Beneficiaries Proof of Address Information**

- Aadhaar Card
- Ration Card
- MNREGA Job Card
- Driving License
- Voter ID Card (EPIC)
- Birth Certificate
- Passport
- PAN Card
- Any other valid government-issued photo ID (to be specified by the state)
- Proof of Relationship (PoR) document

**c) Beneficiaries Health Information**

- Insurance number
- Medical Records/Health Data
- EMR

- EHR
- PHR
- Unique Health Id /Ayushman ID

**d) Financial Details**

- Bank Account Number
- Account Holder Name
- Name of the bank
- IFSC Code of the bank

## 7. Applicable Laws & Regulation

NHA, its ecosystem partners and data principles shall adhere to and comply with all applicable laws, regulations and standards pertaining to privacy as required. Under the current scope of the policy, these include the **Aadhaar Act 2016** and the regulations made thereunder, **Indian Information Technology (Amendment) Act, 2008**, **Right to Information (RTI) Act, 2005** and the rules made thereunder.

## 8. Privacy Principles Adopted by NHA

NHA adopts the following 9 principles to govern the use, collection, and transmission of personal and sensitive personal data of beneficiaries:


**Principle 1: Accountability**
NHA as data Fiduciary shall be accountable for complying with measures which give effect to the privacy principles.

**Principle 2: Openness**
NHA as data Fiduciary, shall make readily available to its employees, beneficiaries, eco system partners specific information about its policies and practices relating to the management of personal data. 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 data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals;

**Principle 3: Choice & Consent**
NHA as data Fiduciary shall give individuals choices (opt-in/opt out) and take individual consent

**Principle 4: Privacy by Design**
NHA shall consider data protection requirements as part of the design and implementation of PM-JAY systems, services, products and business practices.

**Principle 5: Collection Limitation**
NHA as data Fiduciary shall only collect personal data from data principals as is necessary for the purposes identified for such collection. Such collection shall be through lawful and fair means;

**Principle 6: Purpose Limitation**
Personal data collected and processed by data Fiduciarys should be adequate and relevant to the purposes for which it is processed. If there is a change of purpose, this must be notified to the individual. Data retention mandates by the government should be in compliance with the National Privacy Principles;

**Principle 7: Empowerment of Beneficiaries**
NHA believes in strengthening the rights of beneficiaries or data principals in relation to their personal data. Data principal shall be able to seek correction, amendments, or deletion of such data where it is inaccurate; be able to confirm that a data Fiduciary holds or is processing data about them; be able to obtain from the data Fiduciary a copy of the personal data.

**Principle 8: Minimum Necessary Uses & Disclosures**
NHA shall make reasonable efforts to use, disclose, and request only the minimum amount of beneficiaries' personal data needed to accomplish the intended purpose of the use, disclosure, or request. NHA 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**
NHA as data Fiduciary shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against reasonably foreseeable risks;

## 9. Privacy Policy Statements

### 9.1. Governance

**9.1.1.** NHA will be responsible for ensuring the compliance of this Policy in relation to the personal data under its control and shall constitute a committee to be called "**Data Privacy Committee**" headed by a **Data Privacy Officer (DPO).**

9.1.2. The Committee shall have 3 members and be responsible for establishment of Privacy Operation Center (POC) for PMJAY ecosystem, reviewing the compliance with the Data Privacy Policy during the day-to-day operations involving collection and processing of personal data.

9.1.3. DPO will be responsible for

a) Handling privacy issues and concerns regarding the use and disclosure of beneficiaries' personal data and protection of their rights regarding their personal data
b) Defining and documenting a privacy compliance plan and updating the plan at least annually to incorporate changes in its environment ,such as change in PM-JAY program, privacy landscape, legal and regulatory requirements, contracts (including service-level agreements) with service providers, business operations and processes, IT security matters and technology etc.
c) Developing processes to carry out periodic reviews of entire PM-JAY ecosystem, SHA and ecosystem partners to monitor whether processing activities are carried out in line with this policy.
d) Following a risk-based approach towards its Data Privacy program, NHA DPO shall maintain a privacy risk register to document data privacy & protection risks. The privacy risk register shall also document the data privacy risks along with appropriate mitigation plans to remediate the risks. The risk register shall be reviewed periodically by the NHA management.

### 9.2 Privacy Notice

9.2.1. A Privacy Notice shall be made available to data principals in order to refer:

a) At the time or before any data is collected from the beneficiaries, or as soon as practical thereafter, or
b) At the time or before the NHA changes its privacy policies and procedures, or as soon as practical thereafter, or
c) Before data is used for, new purposes not previously identified and notified to the beneficiaries'

9.2.2. The Privacy Notice shall:

a) Specify the type of personal data or sensitive personal data collected by the NHA and its ecosystem partners
b) Specify the mechanisms of collection
c) Specify the purpose(s) of collection and usage of such data
d) Make appropriate disclosures about personal data being shared with third parties
e) Enable the data principals to contact the NHA and its ecosystem partners in regard to complaints, inquiries, and clarifications regarding policies, practices and procedures employed in the collection, storage, and transmittal or processing of personal data

## 9.3 Privacy by Design

9.3.1. NHA and its ecosystem partners shall establish a process to proactively embed privacy as the default state of all products, technologies and services. 'Privacy by Design' principle shall ensure that privacy is considered at the initial planning/design stages and throughout the complete development process of new processes/services/technologies that involve processing of personal data of beneficiaries.

9.3.2. Considerations shall be given for technical and organizational measures to enhance privacy (e.g. **Pseudonymization, anonymization, data minimization** etc.). In addition, appropriate technical and organizational measures shall be considered to ensure that personal data collected or processed is minimal, relevant and limited to what is necessary in relation to the purposes for which it is collected and processed.

9.3.3. Tools to protect the security of personal data must be in-built as per NHA Information Security Policy (NISP).

## 9.4 Choice & Consent

9.4.1. **Choice:** NHA and its ecosystem partners shall, prior collection of data, indicate to the beneficiaries if any of the information is not mandatory for provision of the scheme. For such data, NHA and its ecosystem partners shall provide an option to the data subject to not provide the sought information.

9.4.2. **Consent:** The knowledge and consent of a beneficiary or employee are required for the collection, use or disclosure of personal data, except where inappropriate/ not feasible / not reasonable. Unless any exceptional condition, un-consented data shall not be gathered.

9.4.2.1 The consent of the beneficiaries shall be obtained by using NHA website or mobile application or on paper or any other relevant and appropriate means.

9.4.2.2 The type of consent may be implicit or implied consent or explicit consent. For Aadhaar based authentication and creation of health record of beneficiaries, explicit consent of the data principal is mandatory.

9.4.2.3 The type of consent applicable to a particular situation or process would depend on the business requirement and any specific regulatory or legal requirement;

9.4.2.4 Consent shall be obtained in the language of the individual

9.4.2.5 In the following circumstances, personal data can be collected, used or disclosed without the knowledge and consent of the individual.

a) **Child Consent**: Parent or legal guardian can give consent on behalf a child below the age of 18 years, provided a valid proof of relationship (PoR), proof of identity (PoI) and proof of age of the data principal is submitted.
b) **Beneficiaries who are seriously ill or mentally incapacitated:** In the cases of beneficiaries who are seriously ill or mentally incapacitated, any adult member of the family can give consent, based on proof of relationship (PoR) along with proof of medical condition of the individual

9.4.2.6 **Electronic Consent Framework** notified by Ministry of Electronics & IT (MeitY) is recommended to be adopted for enabling applications to share data about users in a compliant manner.

9.4.2.7 No entity shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.

9.4.2.8 In case of Health records of an individual, every access to each record requires explicit consent of the data principal. NHA must implement Consent Manager in order to ensure that the citizen/ patient as the data principal, is in complete control of what data is collected, and how/with whom it is shared and for what purpose, and how it is processed.

## 9.5 Beneficiary Rights

9.5.1. PM-JAY Beneficiaries shall have the right to:

a) Request access to copies of their personal data
b) Request information on the processing activities carried out with their personal data
c) Request that their personal data is rectified if it is inaccurate or incomplete
d) Request erasure of their personal data in certain circumstances, to be specified by NHA
e) Request that the processing of their personal data is restricted in certain circumstances

f) Object to processing of their personal data in certain circumstances
g) Lodge a complaint with Data Protection Officer of NHA
h) Object to, and not to be subject to a decision based solely on, automated processing (including profiling), which produces legal effects or significant effects on the data principal
i) Withdraw consent

9.5.2. Beneficiaries shall be notified of the cost incurred, if any, in fulfilling such requests
9.5.3. NHA and its ecosystem partners shall not impose any restriction on the method and channel of raising requests by the beneficiaries.

9.5.4. NHA and its ecosystem partners shall not restrict any beneficiary requesting their data based on any characteristics, including language, disability status, technological knowledge, etc.

9.5.5. Managements of NHA and its ecosystem partners shall regularly review the process to ensure all requests raised by beneficiaries are addressed in a timely manner and in compliance with the applicable laws & regulations.

9.5.6. Management of NHA and its ecosystem partners shall oversee the fulfilling of such requests and provide a legal justification in writing (physically or electronically) in case of denial of such requests.

9.5.7. Management of NHA and its ecosystem partners shall maintain records of such requests irrespective of their fulfilling status.

9.5.8. In case of death of the owner of digital health data, the legal heirs or representative of such owner may have access to such data, only upon the application of such heirs or representatives in such form and manner as may be specified by the National Electronic Health Authority of India. Provided that no access shall be given to legal heirs or legal representatives, if it was expressly barred by the owner. Provided further that in case of death of the owner, NHA, shall use the digital health data only in anonymized form.

## 9.6 Limitation of Use and Disclosure of Personal Data

9.6.1. When using or disclosing Beneficiaries' personal data, or when requesting information from any individual or entity, reasonable efforts shall be made to limit the beneficiaries' personal data requested, used, or disclosed to the minimum necessary to accomplish the patient's care.

9.6.2. Identify individuals in its workforce need access to beneficiary's health information and limit access based on job scope and the need for the information.

**9.6.3.** In case of beneficiary's health related purposes mentioned below, only **de-identified or anonymized** data shall be used**.**

a) To improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bioterror events and infectious disease outbreaks;

b) To facilitate health and clinical research and health care quality;
c) To promote early detection, prevention, and management of chronic diseases;
d) To carry out public health research, review and analysis, and policy formulation;
e) To undertake academic research and other related purposes

9.6.4. The data to be shared with the fraud management system shall be **anonymized/ de-identified** to protect privacy of beneficiaries

9.6.5 NHA shall ensure:

a) Appropriate due-diligence covering data privacy and security is carried out prior to on-boarding any new third-party vendor
b) Contracts signed with vendors place adequate security and privacy obligations as well as clear instructions around how personal data shall be handled. A list of liability conditions and other privacy-related conditions that needs to be incorporated into contracts shall also be created and maintained
c) Compliance of vendors to NHA's Information security and privacy obligations is reviewed/ monitored periodically
d) NHA shall clearly notify beneficiaries prior to transfer of their personal data to third party vendors. If not notified previously, the data principal shall be notified prior to performing the transfer and obtain their consent (where necessary)

9.6.6 Personal data shall be shared to third party vendors only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law.

9.6.7 Core biometric information i.e fingerprints and iris, shall not be stored or shared with anyone for any reason whatsoever or used for any purpose other than for authentication.

9.6.8 Aadhaar identity information shall not be—

a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or
b) disclosed further, except with the prior consent of the individual to whom such information relates.

## 9.7 Security Safeguards

NHA and its ecosystem partners shall implement appropriate technical and organizational safeguards, in line with industry standards (such as ISO 27001, ) to ensure the security of personal data, including the prevention of their alteration, loss, damage, unauthorized processing or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment.

9.7.1. NHA has established its information security policies, procedures and guidelines to all employees and any entity forming part of the ecosystem.

9.7.2. NHA, SHA, ecosystem partners or any individual or entity forming part of the PM-JAY ecosystem shall adhere to NHA information security policies, practices and any additional guidance issued by the NHA Information Security Organization (NHA-ISO) and the NHA management while processing personal data.

9.7.3. Confidentiality agreements & NDA's covering data protection and privacy responsibilities shall be signed by all employees & any entity forming part of the ecosystem on or before their joining or induction. Confidentiality agreements shall be reviewed and/or updated/renewed on a periodic basis.

9.7.4. NHA and its ecosystem partners, employees or any entity forming part of the PM-JAY ecosystem involved in any stage of processing Personal Data shall explicitly be made subject to a requirement of secrecy which shall continue for a specified period even after the end of the contractual or employment relationship.

**9.7.5.** Employees or any entity forming part of the PM-JAY ecosystem shall have access only to the personal data necessary for the fulfilment of their employment/ contractual duties based on "need-to-know" principle **(Refer Annexure I).**

9.7.6. Ecosystem partners shall comply with the security safeguards as per its contractual and legal requirements in consultation with NHA-ISO.

9.7.7. NHA-CISO and NHA-DPO jointly shall assess the security measures implemented to safeguard personal data on a regular basis and update the same, where required.

9.7.8. Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.

9.7.9. No entity which is in possession of the Aadhaar number of an Aadhaar number holder, shall make public any database or record containing the Aadhaar numbers of individuals**,** unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form.

9.7.10 No entity shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.

## 9.8 Secure Processing

9.8.1. NHA and its ecosystem partners shall not process personal data in the absence of a valid business and legal basis compliant to applicable laws and regulations.

9.8.2. **Digital health data**, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for a commercial purpose and in no circumstances be accessed, used or disclosed to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as may

be specified by the Central Government (Explanation: Insurance companies shall not insist on accessing the digital health data of persons who seek to purchase health insurance policies or during the processing of any insurance claim.)

9.8.3. **Periodic reviews/audits** shall be conducted to verify and ensure that NHA employees, SHA and all ecosystem partners collect/process personal data appropriately in compliance with privacy notices, contracts and this policy.
9.8.4. NHA and its ecosystem partners shall maintain records to document the processing activities under its responsibilities in form of **Personal Data Inventories** and **Data Flow Diagrams (DFD's)**. Those documented records shall cover the following:

a) Details of the ecosystem partners
b) Purposes of the processing
c) Description of the categories of data principals
d) Description of the categories of personal data
e) Categories of recipients to whom the personal data is disclosed/ transferred including third parties
f) Geographies of recipients

9.8.5. Individual(s)/ entities handling personal data of beneficiaries shall develop, maintain and update their Personal data inventories and DFD's. The Personal data Inventories and DFD's shall be reviewed and updated periodically (at minimum semi-annually) or in the event of any significant changes to the processing activities

## 9.9 Audit Trail

9.9.1. A strict audit trail shall be maintained of all activities which have read or write access to beneficiaries personal data, at all times, and may be reviewed by an appropriate authority like auditor, legal representatives of the patient, the patient, healthcare provider, privacy officer, court appointed/authorized person, as deemed necessary.

## 9.10 Data Breach or Incident Management

9.10.1. NHA shall formulate and implement an incident and breach management mechanism to ensure that exceptions in data privacy compliance are promptly reported to the incident response team of NHA and its ecosystem partners.

9.10.2. All employees or any entity forming part of the PM-JAY ecosystem shall be aware of the mechanism of raising alerts and notifications on data privacy and security incidents.

9.10.3. The NHA Data Privacy Committee shall work closely with the incident response team, ecosystem partners and NHA Information Security teams (plus Legal and senior management where appropriate) to investigate potential data privacy and data breach incidents and track to closure.

9.10.4. NHA and its ecosystem partners shall maintain an inventory of such incidents and shall record the lessons learnt

9.10.5. NHA ecosystem partners shall ensure that timely notification of breaches is provided to NHA and data principals. NHA shall notify the time limits within which incidents of different levels of severity shall be so reported.

9.10.6. Documented procedures shall be maintained to identify, track, review and investigate incidents to identify potential data breaches. As applicable, the NHA shall take actions to notify the data principals and eco system partners.

9.10.7. For any Privacy breach, following a breach of unsecured protected health information or unauthorized disclosure of beneficiaries' information, NHA must provide notification of the breach to Cert-In, affected individuals if necessary and in certain circumstances, to the media. In addition, eco system partners must notify that a breach has occurred.

## 9.11 Data Retention and Disposal

9.11.1. Personal Data shall not be retained longer than required for the purpose it was collected for, or as defined by the NHA Information Security Policy (NISP), after considering the regulatory requirements.

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

9.11.3. Personal Data shall only be erased if their storage violates any of the data protection principles or if knowledge of the data is no longer required by NHA and its ecosystem partners or for the benefit of the beneficiary.

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

9.11.5. Disposal of personal data shall be handled with utmost care and shall be governed by the NHA Information Security Policy (NISP).

9.11.6. Where third parties are disposing of personal data on behalf of NHA and its ecosystem partners a certificate or other notification of the destruction shall be required.

## 9.12 Training & Awareness

9.12.1. Training & awareness materials around data protection and privacy shall be developed for NHA employees and entire ecosystem partners. NHA shall also develop role-based trainings for individuals or teams considering their role and nature of processing.

9.12.2. Data Privacy training and awareness programs shall be conducted on a periodic basis (at minimum annually) for all employees and contractors working at NHA.

9.12.3. Training attendance records shall be maintained for documentation and audit purpose.

## 10. Grievances and Compliant Redressal

NHA shall **maintain procedures for addressing and responding to all inquiries or complaints** from beneficiaries and employees about the handling of personal data

a) NHA shall inform their beneficiaries about the existence of these procedures as well as the availability of complaint procedures
b) The Individual(s) accountable for compliance with the NHA Data Privacy Policy may seek external advice where appropriate before providing a final response to individual complaints

Beneficiaries/data principals with inquiries or complaints about the processing of their Personal Data shall first report the matter to the **NHA Data Privacy Officer (NHA-DPO)** in writing or email ID provided under grievance portal of PM-JAY website (https://www.pmjay.gov.in/) The details of the NHA Data Privacy Officer shall be displayed on the PM-JAY website (https://www.pmjay.gov.in/) always along with the contact details and the format and process for filing the grievances. Any disputes concerning the processing of the Personal Data of beneficiaries will be resolved through arbitration.
If an issue is not resolved through consultation with NHA management, or through other mechanisms under existing agreements, union agreements, or statutory procedures, then the beneficiary may, at its option, seek redress through resort to mediation, binding arbitration, litigation, or complaint to **Ministry of Health & Family Welfare (MoHFW)** with jurisdiction.

## 11. Compliance

Data Privacy Officer (DPO) of NHA shall ensure adherence to this policy and shall be responsible for appropriate remedial action. All individuals or entities who are covered by this Policy must comply with it, and where requested demonstrate such compliance. Failure to comply with this policy can result in disciplinary action which may include termination of services of employees or termination of the engagement of a consultant/contractor/service provider or dismissal of interns or volunteers. This is without prejudice to the action that can be initiated under the applicable law.

## 12. Penalty for Non-compliance

Whoever, fails to comply with the requirements of this policy, shall be punishable with a fine which may extend to ten thousand rupees or, in the case of an ecosystem partner of PM-JAY may extend to one lakh rupees.

Non-compliance o this policy may also result in blacklisting of an individual or the respective ecosystem partner.

## 13. Policy Governance

NHA management shall be responsible for compliance with all applicable legal & regulatory requirements such as the Aadhaar Act & IT Act for safeguarding beneficiaries' personal data.

a) NHA management shall implement formalized processes to track and address any inquiries and complaints received from beneficiaries in a timely manner
b) This Policy shall be revised at least once in a year. This policy and any significant revisions shall be provided to all beneficiaries, employees and any agency part of the ecosystem through the website of NHA

## Annexure I

| **Oral Conversations – in person** | **Courier and Regular Mail** |
|---|---|
| a) Discuss beneficiaries' sensitive data in private. Use an office with a door whenever possible, or avoid areas where others can overhear.<br>b) Be aware of those around you and lower your voice when discussing beneficiaries' sensitive personal data.<br>c) If possible, point out sensitive personal data on paper or on-screen nonverbally when discussing beneficiaries sensitive personal data.<br><br>**Oral Conversations – telephone**<br><br>a) Follow the above guidelines for "Oral Conversations"-in person"<br>b) Don't use names- instead say; "I have a question about you/ beneficiaries".<br>c) Never give sensitive personal data over the phone when talking to unknown callers, but call back and confirm the identity of the caller.<br>d) Never leave sensitive personal data on voice messages; instead leave a message requesting a return call to discuss a participant giving only your name and phone number.<br>e) Do not discuss sensitive personal data over unencrypted cellular or portable (wireless) | a) Use sealed secured envelopes to send sensitive personal data.<br>b) Verify that the authorized person has received the package.<br>c) Deliver all mail promptly to the recipient.<br>d) Mailboxes must be in safe areas and not located in public or high-traffic areas.<br><br>**Inter-Office Mail (Within the same organization)**<br><br>a) Put sensitive personal data in closed inter-office envelopes. As an added precaution, put sensitive personal data in a sealed envelope inside the inter-office envelope.<br>b) Identify recipient by name and verify mail center address.<br>c) Distribute inter-office mail promptly to recipients. Do not leave unattended in mailboxes.<br>d) Where practical, use lockable containers (e.g. attaches) to transmit correspondence that contains participant sensitive personal data.<br><br>**Computer Workstations** |

phones or in an emergency, as the transmissions can be intercepted.

**Fax**

a) Put fax machines in a safe location, not out in the open or in a public or area with high-traffic or easy access and visibility.
b) Use a cover sheet clearly identifying the intended recipient and include your name and contact information on the cover sheet.
c) Include a confidentiality statement on the cover sheet of faxes that contain sensitive personal data.
d) Do not include or reference sensitive personal data on cover sheet.
e) Confirm fax number is correct before sending.
f) Send fax containing participant sensitive personal data only when the authorized recipient is available to receive it whenever possible.
g) Verify that fax was received by authorized recipient; check the transmission report to ensure correct number was reached and when necessary contact the authorized recipient to confirm receipt.
h) Deliver received faxes to recipient as soon as possible. Do not leave faxes unattended at fax machine.

**Email**

a) Do not include sensitive personal data in Subject-line or in Body of email.
b) Transmit sensitive personal data only in a password-protected attachment (MS Word and MS Excel provide password protection).
c) Include a confidentiality statement on emails that contain any sensitive personal data in email attachments.
d) Do not send attachment passwords in the same email as the attachment.
e) Include your contact information (name and phone number minimum) as part of the email.

a) Use password protected screen savers, turn off the computer, or log out of the network when not at your desk.
b) Position screens so they are not visible to others.
c) Secure workstations and laptops with password.
d) Change passwords on a regular basis.
e) Do not leave laptop or work-related participant sensitive personal data visible or unsecured in a car, home office, or in any public areas.
f) Ensure that all sensitive personal data used outside work premises is protected using appropriate measures such as locked desks, file cabinets.
g) Never remove original copies of sensitive personal data from the agency without your supervisor's approval for specific purposes.
h) Store files that contain sensitive personal data on a secure server, not on your workstation hard drive.

**Disposal of sensitive personal data**

a) Shred all hard copies containing sensitive personal data when the copies are no longer needed.
b) Place hardcopies to be recycled in locked recycle bins if available.
c) Delete all soft copy files containing sensitive personal data from your computer and from the server when the information is no longer needed within the record retention requirements.
d) Destroy all disks, CDs, etc., that contained sensitive personal data before disposing them.
e) Do not reuse disks, CDs that contained sensitive personal data without sanitizing them first.
f) Contact IT before transporting or transferring equipment for proper procedures to move equipment and to sanitize hard drives and other media.
g) Return the sensitive personal data to the sender, if this requirement is stipulated in any contractual agreements. Work Areas
h) Do not leave sensitive personal data (files, records, Rolodex, reports) exposed, open, or

| | |
|---|---|
| f) Set email sending options to request an automatic return receipt from your recipient(s).<br>g) Request that email recipients call to discuss specific participant data.<br>h) Do not store emails or email attachments with sensitive personal data on your hard drive but copy and store to a secure server. Delete the email and the attachments when they are no longer needed. | unattended in public areas, conference rooms, mailboxes, wall trays, etc.<br>i) Store all sensitive personal data securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area. |