NHA Data Sharing Guidelines

PRADHAN MANTRI JAN AROGYA YOJANA (PM-JAY)

July 2022

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 interrelated components, which are -

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

PM-JAY 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. HWCs, 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 PM-JAY is to adopt cooperative federalism and provide flexibility to states. For giving policy directions and fostering coordination between Centre and States, Pradhan Mantri Jan Arogya Yojana Council (PM-JAYC) has been set up at the apex level and it is chaired by Union Health and Family Welfare Minister.

NHA 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 a 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 personal and sensitive personal data.

2. Purpose

NHA (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 PM-JAY.

These Data Sharing Guidelines outlines how NHA and its ecosystem partners collect, process, and use personal data of beneficiaries and complies with the Aadhaar (Targeted Delivery of Financial and Other Subsidies, benefits and Services) Act, 2016 (Aadhaar Act); the Information Technology Act, 2000 (IT Act) and the Right to Information Act, 2005 (RTI Act) and rules and regulations thereunder. These guidelines set out the minimum standard and shall guide all NHA employees and its ecosystem partners.

These guidelines are to be read with, and not in contradiction to any applicable law, or any instrument having the force of law, and 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 having the force of law.

3. Applicability

The provisions of these Guidelines shall be applicable to the employees of the NHA (NHA), the State Health Agency(ies), hospitals, health insurance providers, health service consultants and any individuals, entities, or ecosystem partners who collect or process personal data of beneficiaries or of individuals for the purpose of implementing PM-JAY schemes, or are involved in the collection, use, disclosure, retention and storage of personal data as part of a PM-JAY scheme.

4. Objective

The key objectives of these guidelines are to:

a. provide an adequate guidance framework for the secure handling of the personal data and personal data of the beneficiaries of the schemes constituted under the PM-JAY in compliance with laws that are in force and applicable to NHA and entities in the NHA ecosystem.

b. increase awareness regarding the importance of privacy and data protection as well as to instill a privacy-oriented mind-set among the members of NHA and its ecosystem partners

c. safeguard personal data, including sensitive personal data of the beneficiaries , by implementing adequate technical and organizational measures.

d. establish appropriate institutional mechanisms for auditing of the ecosystem as needed, to ensure appropriate compliance by all stakeholders with these data sharing guidelines

e. establish an institutional mechanism for sharing data with any entity requesting data for specific purposes as defined under these guidelines.

5. Mechanisms for Collection of Personal Data

a. NHA and its ecosystem partners may collect personal or sensitive personal data from beneficiaries only after obtaining their consent as set out under Clause 9.4 below.
b. NHA and its ecosystem partners may collect personal data from various sources such as SECC, RSBY, State/ Central databases and/or from the NHA's Information Technology Framework which may involve components including but not limited to HEM, TMS, BIS, dashboards.
c.

6. Type of Personal andSensitive Personal Data Collected

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

a) Identity Information of beneficiaries 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) Proof of Address Information of beneficiaries

- 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) Health Information of beneficiaries

- Insurance number
- Medical Records/Health Data
- EMR
- EHR
- PHR
- ABHA

d) Financial Details

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

7. Applicable Laws

All entities to which these Guidelines are applicable shall adhere to and comply with all applicable laws, 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.

These Guidelines are to be read along with, and not in contradiction to, any applicable law, or any instrument having the force of law, including any other policies or guidelines which may be notified from time to time by the NHA. 8. Privacy Principles Adopted by NHA

Subject to the provisions of applicable laws, NHA will follow the below principles to govern the use, collection, processing and transmission of personal or 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. However, the control of personal data will remain with the beneficiaries.

Principle 2: Openness/ Transparency

NHA as data Fiduciary, shall make readily available to its employees, beneficiaries, ecosystem 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 and Consent

NHA as a data fiduciary shall give individuals a choice to opt-in/opt-out of its schemes and obtain their consent prior to accessing, sharing or processing any of their personal data. The consent should be free, informed, clear, and specific.

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. NHA shall also prepare and publish a privacy by design policy which may contain information such as: the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal; the obligations of data fiduciaries; the technology used in the processing of personal data, in accordance with commercially accepted or certified standards; the protection of privacy throughout processing from the point of collection to deletion of personal data; the processing of personal data in a transparent manner; and the fact that the interest of the data principal is accounted for at every stage of processing of personal data. Tools to protect the security of personal data must be in-built as per NHA Information Security Policy (NISP).

Principle 5: Collection, Use, and Storage Limitation

NHA as data fiduciary shall only collect personal data from data principals as is necessary for the purposes identified for such collection and will use the personal data in the manner for the purpose for which it was collected. The processing of personal data will be in a fair and reasonable manner, ensuring the privacy of the data principal. The personal data shall not be retained for a period beyond which it is necessary to satisfy the purpose for which it was collected. The data fiduciary shall delete such personal data in accordance with guidelines pertaining to data retention as may be issued by the NHA from time to time.

Principle 6: Purpose Limitation

All personal data collected and processed by data fiduciaries should be for a specific, lawful and clear purpose as may be identified in the privacy notice issued by the NHA as data fiduciary and should be consented to by the data principal.

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 and 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: Reasonable Security Safeguards and Procedures

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. Data Sharing Guideline Statements

9.1. Governance

9.1.1. NHA will be responsible for ensuring the compliance of these guidelines in relation to the personal data under its control and shall constitute a committee to be called "Data Sharing Committee" headed by a Data Sharing Officer (DSO).

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

9.1.3. DSO 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 the entire PM-JAY ecosystem, SHA and ecosystem partners to monitor whether processing activities are carried out in line with these guidelines.
d. Following a risk-based approach towards its Data Sharing program, NHA DSO shall maintain a data sharing risk register to document data sharing and data protection risks. The data sharing risk register shall also document the data sharing risks along with appropriate mitigation plans to remediate the risks. The risk register shall be reviewed periodically by the NHA management.
e. Handling requests for access to personal data under these guidelines.

9.2 Privacy Notice for the collection or processing of personal data

9.2.1.
The NHA as data fiduciary shall give a clear and conspicuous Privacy Notice, in such form as may be specified by the NHA, to the data principals:
(a) Prior to the collection of personal data from the data principal; and
(b) Prior to the collection or further processing of personal data of the data principal for any new or previously unidentified purpose.

9.3 Privacy Policy

9.3.1 NHA will also prepare and publish a privacy policy in relation to personal data collected by it, containing information such as: clear and easily accessible statements of its practices; types of sensitive personal data and personal data collected; purpose of collection and usage of such personal or sensitive personal data; whether such personal or sensitive personal data is being shared with other data fiduciaries; reasonable security practices and procedures that are in use to safeguard the personal data being processed.

9.3.2. The Privacy Policy referred to in Clause 9.3.1 shall:

a. Provide a clear and easily accessible statement of the practices and policies followed by NHA in relation to personal data under these Guidelines
b. Specify that personal data including Sensitive Personal Data is being collected by the NHA and its ecosystem partners
c. Specify the purpose(s), as under Clause 9.6.3, of collection and usage of such data
d. Make appropriate disclosures about personal data being shared with third parties
e. Specify the reasonable security practices and procedures in relation to such personal data

9.4 Choice and 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 necessary under any law in force for the time being.

9.4.2.1 The informed consent of the beneficiaries shall be obtained in accordance with Rule 5 Sub Rule 1 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, the beneficiary also shall have the right at all times to withdraw this consent.

Where the data principal withdraws his consent from the usage/ processing of any personal data, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

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

a. Consent on behalf of a child: Parent or legal guardian can give consent on behalf of 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
c. Anonymized Data
d. NHA as the data fiduciary may disclose protected health information to a Government agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions.
e. Epidemics declared/ notified diseases under the Epidemic Diseases Act and amendments thereof.

NHA as the data fiduciary may disclose protected health information in the course of any judicial or administrative proceeding and/ or in response to an order of a court or administrative tribunal, provided that the NHA as data beneficiary discloses only the protected health information expressly authorized by such order..

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

9.4.2.4 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 in compliance with Aadhar Act.

9.4.2.5 In the case of Health records of an individual, every access to each record requires explicit consent of the data principal. NHA must put in place a data release mechanism 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 can request the following from the data fiduciaries:

a. Confirmation and access
    a. Request access to copies of their personal data processed by the data fiduciary; and
    b. Request information on the processing activities carried out with their personal data, including accessing in one place, the identities of the entities with whom his/her personal data has been shared by the data fiduciary together with the categories of personal data that has been shared

c. Correction and erasure
d. Request that their personal data is rectified if it is inaccurate or incomplete
e. Request erasure of their personal data in certain circumstances, to be specified by NHA, in accordance with these guidelines and any applicable law in force for the time being

b. Restrict or object to disclosure
   a. Request that the processing of their personal data is restricted in certain circumstances as may be specified by the NHA
   b. Object to processing of their personal data in certain circumstances as may be specified by the NHA

c. Lodge a complaint with Data Sharing Officer of NHA
d. 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
e. Withdraw consent in accordance with the provisions of applicable laws

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. The NHA and its ecosystem partners shall regularly review and overview the process to ensure all requests raised by beneficiaries are addressed in a timely manner and in compliance with the applicable law currently in force. In the event that the NHA or its ecosystem partners is unable to fulfill such a request then the NHA or the ecosystem partner provide a justification for the same.

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

9.5.7. In case of death of the owner of 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 Health Authority.

9.6 Limitation of Purpose, 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 by the data fiduciary to limit the beneficiaries' personal data requested, used, or disclosed to the minimum necessary to accomplish the purposes referred to in Clause 9.6.3.

9.6.2 All requests for access to personal data of beneficiaries must be made through the designated authority by the NHA, which by default is the Data Sharing Committee constituted under Clause 9.1 of these Guidelines

Provided that the Decision of the Data Sharing Committee in respect of any request for access to personal data shall be final and there shall be no provision of any appeal.

9.6.3. The purposes for the collection or processing of personal data shall be limited to such purposes as may be specified by the NHA, and such purposes shall be related to the beneficiaries health, provision of care or services to the beneficiaries and such other incidental purposes which a data principal can reasonably expect, having regard to the purpose, context and circumstances in which the personal data was collected or processed.

9.6.4 Every data fiduciary shall identify the individuals in its workforce who require access to beneficiary's health information under these Guidelines for the purposes referred to in Clause 9.6.2, and shall limit access to personal data based on the job scope and the need for the information, in accordance with these Guidelines and any applicable law in force for the time being.

9.6.5. In the case of purposes mentioned below, only de-identified or anonymized data shall be used under these Guidelines:

a. Improving public health activities and facilitating the early identification and rapid response to public health threats and emergencies, such as infectious disease outbreaks and other such threats and emergencies;
b. Facilitating health and clinical research and health care quality;
c. Promoting early detection, prevention, and management of chronic diseases;
d. Carrying out public health research, review and analysis, and policy formulation;
e. Undertaking academic research and other related purposes

9.6.6. Anydata related to the beneficiaries shared with any systems implemented by the NHA for the purpose of detection and prevention of fraud as may be specified, shall be anonymized/ de-identified to protect privacy of beneficiaries

9.6.7 NHA shall:

a. Ensure appropriate due-diligence covering data privacy and security is carried out prior to on-boarding any new third-party vendor in relation to personal data under these Guidelines
b. Incorporate adequate security and privacy obligations, as well as clear instructions around how personal data shall be handled in any contracts signed with vendors
c. Create and maintain a list of liability conditions and other privacy-related conditions that needs to be incorporated into contracts with third-party vendors
d. Review/monitor periodically the compliance of vendors to NHA's Information security and privacy obligations

e. Clearly notify beneficiaries prior to transfer of their personal data to third party vendors in accordance with these Guidelines and any applicable law in force for the time being. If not notified previously, the data principal shall be notified prior to performing the transfer and where necessary or required, their consent for the same shall be obtained

9.6.8 Personal data shall be shared to third party vendors only for reasons consistent with the purposes under Clause 9.6.2 for which the data were originally collected, or other purposes authorized by law.

9.6.9 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 in accordance with the provisions of the Aadhaar (Targeted delivery of financial and other subsidies, benefits and services) Act, 2016 and the regulations made thereunder.

9.6.10 Any information processed for the authentication of the beneficiaries under the Aadhaar Act and the regulations made thereunder shall not be—

a. used for any purpose, other than that specified to the individual at the time of submitting any information for authentication; or
b. disclosed further, except with the prior consent of the individual to whom such information relates in accordance with these Guidelines and any applicable law in force for the time being.

9.7 Security Safeguards

9.7.1 NHA and every entity to whom these Guidelines are applicable shall implement appropriate managerial, technical, physical, operational 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.

9.7.2. NHA shall notify the information security policies, procedures and guidelines which shall be applicable to all employees and any entity forming part of the ecosystem.

9.7.3. NHA, and 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 while processing personal data.

9.7.4. Confidentiality agreements and Non-disclosure agreements covering data protection and privacy responsibilities shall be signed by all employees of NHA, and any entity forming part of the ecosystem on or before their joining or induction, as the case may be. Confidentiality agreements shall be reviewed and/or updated/renewed on a periodic basis.

9.7.5. 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 in relation to any personal data referred to in these Guidelines, 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 fulfillment of their employment/ contractual duties based on "need-to-know" principle in accordance with these Guidelines and the provisions of any applicable law (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

9.7.7. NHA 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 legal basis in accordance with these Guidelines and in compliance with applicable laws and regulations in force for the time being.

9.8.2. Any health data under these Guidelines, whether identifiable or anonymized, shall not be accessed, used or disclosed to any person for any 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.

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, any applicable contracts and these guidelines.

9.9 Audit Trail

9.9.1. A strict audit trail shall be maintained by every data fiduciary under these Guidelines 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, sharing officer, court appointed/authorized person, as deemed necessary.

9.9.2 The audit trail shall include the following records, and any other records or information as may be specified by the NHA:

a. a record of all processing activities which have access to personal data
b. a record of how such personal data is processed or used
c. 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 were disclosed

9.10 Sharing of anonymised and de-identified data

9.10.1 NHA shall make aggregated and anonymised data available through a public dashboard 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

9.10.2 NHA shall specify the terms under which the anonymised data shall be made available through the public dashboard, including terms in relation to the use of such data and the manner in which such data may be accessed.

9.10.3 NHA shall set out a procedure through which anonymised or de-identified data may be made available to any entity seeking such information for the purposes referred to in Clause 9.10.1, where such entity may make a request to the Data Sharing Committee for the sharing of such information through secure modes, including clean rooms and other such secure modes specified by NHA

9.10.4 NHA shall specify the terms under which anonymised or de-identified data shall be made available through secure modes under 9.10.3, including terms in relation to the access and use of such data and the manner in which it may be accessed.

9.10.5 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 being anonymised or de-identified.

9.10.6 The anonymisation or de-identification of data shall be done by NHA in accordance with technical processes and anonymisation protocols which may be specified by the NHA

9.11 Data Breach or Incident Management

9.11.1. NHA shall formulate and implement a personal data breach management procedure, which shall be publicly displayed. Every data fiduciary under these Guidelines shall ensure that any instance of non-compliance with the provisions of these Guidelines, 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 the Data Sharing Committee and 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

9.11.2 All cyber security incidents shall be reported to the Data Sharing Committee and adjudicated upon by the Data Sharing Committee. The Data Sharing Committee shall have the authority to take actions under any law for the time being in force in relation to such breach as it may deem fit.

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

9.11.4. The Data Sharing 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 such incidents to closure.

9.11.5. NHA and its ecosystem partners shall maintain an inventory of such incidents and shall record the decision of the Data Sharing Committee on every such incident, and the actions taken pursuant to such decision.

9.11.6. 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 .

9.11.7. NHA ecosystem partners shall ensure that timely notification of breaches is provided to NHA and, where specified by the NHA, to the data principals. NHA shall notify the time limits within which incidents of different levels of severity shall be so notified.

9.11.8. Documented procedures in accordance with applicable law 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 ecosystem partners.

9.12 Data Retention and Disposal

9.12.1. Personal Data shall not be retained longer than required for the purpose it was collected for or as otherwise required under any other law in force for the time being..

9.12.2. Personal Data shall be blocked and restricted, rather than erased, insofar as the law prohibits erasure, where the 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. Where erasure is not possible without disproportionate effort due to the specific type of storage, overwriting, anonymization or other method(s) of removal of the data from live systems shall be used.

9.12.3. Personal Data shall be erased if its storage violates any of the data protection principles under these Guidelines, or if the data is no longer required by NHA and its ecosystem partners, or for the benefit of the beneficiary.

9.12.4. Disposal of personal data shall be handled with utmost care and shall be governed by the NHA as per its policies and the provisions of any applicable law.

9.12.5. Where third parties are disposing of personal data on behalf of NHA and its ecosystem partners, a certificate or other notification of the destruction in such manner as may be specified by the NHA shall be required.

9.13 Training and Awareness

9.13.1. Training and 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.

9.13.2. Training and awareness programs in relation to data sharing and protection shall be conducted on a periodic basis (at minimum annually) for all employees and contractors working at NHA.

9.13.3. Training attendance records shall be maintained for documentation and audit purposes.

10. Grievances and Complaint Redressal

10.1 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 Sharing Guidelines may seek external advice where appropriate before providing a final response to individual complaints

10.2 Beneficiaries or data principals with inquiries or complaints about the processing of their Personal Data, or in relation to any contravention of these Guidelines or any other applicable law in force for the time being, may report the matter to the NHA Data Sharing Officer (NHA-DSO) in writing or email ID provided under grievance portal of PM-JAY website (https://www.pmjay.gov.in/) The details of the NHA Data Sharing 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.

10.3 The NHA Data Sharing Officer shall acknowledge any complaints received by it within a period of [-] days from the receipt of such complaint, and shall redress such grievances within [one month] from the date of receipt of such complaint.

10.4 If an issue or grievance is not resolved by the NHA Data Sharing Officer, or 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 or remedy in accordance with any applicable laws in force for the time being, and where applicable, may make a complaint regarding such grievance to Ministry of Health and Family Welfare (MoHFW).

11. Compliance

Data Sharing Committee (DSC) of NHA shall ensure adherence to these guidelines and shall be responsible for appropriate remedial action. All individuals or entities who are covered by these guidelines must comply with it, and where requested by the NHA, demonstrate such compliance.

Failure to comply with these guidelines 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

12.1 Whoever, fails to comply with the requirements of these guidelines, shall be liable for such non-compliance under any applicable laws in force for the time being. .
\12.2 Non-compliance of any entity with these guidelines may also result in blacklisting of an individual or the respective ecosystem partner, and their removal from the PM-JAY ecosystem. The Data Sharing Committee shall be the final adjudicating authority in this matter.

13. Guideline Governance

NHA shall be responsible for compliance with all applicable legal and regulatory requirements such as the Aadhaar (Targeted delivery of financial and other subsidies, benefits and services) Act, 2016 and the Information Technology Act, 2000 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. These guidelines shall be revised from time to time as and when need arises. These guidelines and any significant revisions shall be provided to all beneficiaries, employees and any agency part of the ecosystem through the website of NHA

14. Definitions

a. "Authentication" shall have the meaning assigned to it under clause (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

b. "Arogya Mitras" are facilitators to be placed in each hospital empaneled 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.

c. "Anonymization", in relation to personal data, means the 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. "Beneficiary" means any eligible beneficiary identified under PM-JAY

e. "Biometric Information" means the information from technologies that measure and analyses human body characteristics, such as but not limited to 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', and 'DNA' for authentication purposes;

f. “Clean room” refers to a secure sandboxed area, with access controls, where aggregated and anonymised or de-identified data may be shared for the purposes of developing inference or training models.

g. “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, as referred to in Clause 9.4.

h. Covered Entity- Means an entity/ organization covered under these guidelines in accordance with Clause 3.0.

i. “Data” shall have the meaning assigned to it under clause (o) of sub-section (1) of section 2 of the Information Technology Act, 2000

j. “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 these guidelines, data fiduciary includes the NHA.

k. “Data Principal” means the natural person to whom the personal data relates, and shall include beneficiaries.

l. “De-identification” means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to a data principal but does not, on its own, directly identify the data principal;

m. “Electronic 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. It shall be deemed to be equivalent to a physical consent for the purposes of these guidelines.

n. “Electronic Medical Record (EMR)” refers to a repository of records that is stored and used by the data fiduciary or any other entity generating such records to support patient diagnosis and treatment. EMR may be considered as a special case of EHR, limited in scope to the medical domain or is focused on the medical transaction.

o. “Electronic Health Record (EHR)” are one or more repositories, physically or virtually integrated, of data in digital form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users (such as 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.

p. “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.

q. “Personal data” means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;

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

s. “Personnel” includes all officers, employees, staff and other individuals employed or engaged by NHA or by the service providers supporting PM-JAY ecosystem.

t. “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.

u. “Re-identification” means the process by which a data fiduciary or data processor may reverse a process of deidentification;

v. "Sensitive personal data" shall have the meaning assigned to it under Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, and shall include any other data categorised as sensitive personal data by any notification from NHA .

w. “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.

x. “Health ID (UHID)” is an identifier for each patient or beneficiary that serves as a key to a patient’s or beneficiary’s health record. Further details on it can be referred in the National Digital Health Blueprint (NDHB) published by the Ministry of Health and Family Welfare (MoHFW).

Annexure-1

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

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. f) Set email sending options to request an automatic return receipt from your recipient(s). g) Request that email recipients call to discuss specific participant data. 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.	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 Unattended in public areas conference room mailboxes wall trays etc i) Store all sensitive personal data in locked file cabinets desk drawers offices or suites when you are not in your work area.

Document Control

Type of Information	Document Data
Document Title	NHA Data Sharing Guidelines
Document version	2.0
File No	S-12019/33/2019-NHA
Document Owner	National Health Authority (NHA)
Advisors	Shri J Satyanarayana, Advisor, NHA
Document Number	PMJAY-IS-DOC-12

Document Approver

Version	Date of Approval	Approved By	Name
1.0	27 Aug 2018	CEO, NHA Dy. CEO, NHA	Dr. Indu Bhushan Dr. Dinesh Arora
2.0	20 July, 2020	CEO, NHA	Dr. Indu Bhushan
3.0	13 June, 2022	CEO, NHA	Dr R S Sharma

Revision Change History

Version	Date	Prepared By / Modified By	Significant Changes
1.0	27 Aug 2018	NHA IS team	Initial documentation

2.0	11 July, 2020	NHA IS team	• Logo Updated • Consent manager added under section 9.4.2.8 • Penalty for Non-compliance added under Section 12
3.0		NHA	• Title changed to Data Sharing Guidelines • Powers of DSC expanded • Security Safeguard strengthened. • Clean room and differential privacy concept introduced • Exceptions to policy updated.