Data Privacy, Confidentiality, Anonymization, and Data Sharing

GRID Council

Standard Operating Procedure (SOP)

SOP for Data Privacy, Confidentiality, Anonymization, and Data Sharing
Version 1.0; January 2026

Data Privacy, Confidentiality, Anonymization, and Data Sharing, GRID Council

Standard Operating Procedure (SOP)

A. SOP Details

Organization Name:	Generating Research Insights for Development (GRID) Council
GRID Council- SOP Name	Data Privacy, Confidentiality, Anonymization, and Data Sharing
Document Number:	Policy/HR/01
Policy effective date (DD-MM-YYYY):	01-01- 2026;
Last Revised on (DD-MM-YYYY):	-
Version Number:	1.0
Total number of pages	07
Total number of annexures	01

B. SOP Prepared by

Name & Designation	Signature
Hamza Salah (Senior research assistant)	Hamza salah

C. SOP Reviewed by

Name & Designation	Signature
Ritika Mukherjee (Deputy director)	Ritika mukherjee

D. SOP Approved by

Name & Designation	Signature
Archisman Mohapatra (Executive Director)	Archisman mohapatra

Table of Contents

1. Purpose

This Standard Operating Procedure (SOP) describes the principles, processes, and safeguards governing the collection, storage, processing, anonymization, and sharing of health-related research data generated through projects implemented by GRID Council in India, including projects undertaken in collaboration with international partners.

This SOP is intended to ensure compliance with applicable Indian laws and ethical guidelines, while being aligned with internationally accepted data protection principles.

2. Scope

This SOP applies to all GRID Council–led or GRID Council–affiliated research activities that: - Involve primary or secondary data collection from hospitals or health facilities in India; - Include personal data, sensitive personal data, or health-related data; - Require sharing of processed or derived datasets with collaborators outside India.

The SOP applies from the point of data collection through data archiving and regulated data sharing.

3. Regulatory and Ethical Framework

This SOP has been developed in accordance with the following:

3.1 Indian Legal and Ethical Framework

- **ICMR National Ethical Guidelines for Biomedical and Health Research Involving Human Participants (latest edition)**
- **Digital Personal Data Protection (DPDP) Act, 2023 (India)**
- **Digital Information Security in Healthcare Act (DISHA)**, where applicable, and as a guiding framework for health data governance
- Conditions specified by relevant Institutional Ethics Committees (IECs)

3.2 International Alignment

While primary compliance is with Indian law, this SOP is aligned with internationally accepted data protection principles reflected in: - **General Data Protection Regulation (GDPR) –** including lawfulness, fairness, data minimization, purpose limitation, and security - **Health Insurance Portability and Accountability Act (HIPAA) –** including administrative, technical, and physical safeguards for health data

Such alignment is intended to facilitate international collaboration and does not imply transfer of identifiable personal data outside India.

4. Roles and Responsibilities

- **Principal Investigator (India):** Overall accountability for data governance, compliance with law and ethics approvals, and authorization of data access.
- **Data Manager (India):** Responsible for secure data handling, access control, anonymization, documentation, and audit readiness.
- **Authorized Research Staff (India):** Data collection and processing strictly in accordance with approved protocols and this SOP.
- **International Collaborators:** Access limited strictly to anonymized, processed datasets, subject to a Data Sharing Agreement.

5. Data Collection Platforms

5.1 Platform Selection Principles

GRID Council adopts a **risk-proportionate, technology-agnostic approach** to electronic data capture. The choice of platform is guided by: - Sensitivity and identifiability of data collected; - Scale and complexity of the study; - Requirements of ethics committee approvals; - Practical considerations related to accessibility, training, and feasibility.

No Indian law or ethical guideline mandates the use of a specific data collection software for health research. Compliance is determined by the safeguards implemented, rather than the brand or origin of the platform.

5.2 Primary Platform: Google Forms

- As a general practice, GRID Council will use **Google Forms** for collection of low- to moderate-risk research data.
- Google Forms provides encrypted data transmission and storage, access control through authenticated user accounts, and administrative security controls.
- Access to forms and responses will be restricted to authorized GRID Council personnel based in India.
- Data elements collected will be limited to those necessary for the approved research objectives.

The use of Google Forms, when combined with appropriate organizational, technical, and procedural safeguards, is **legally permissible and compliant with Indian data protection requirements**, including the DPDP Act and ICMR ethical guidelines.

5.3 Alternative Platforms (as Appropriate)

Depending on study requirements, GRID Council may also use: - **REDCap** (institutionally hosted or cloud-hosted); - **ODK-based tools** (e.g., ODK Collect, KoBoToolbox, Epicollect); - Other secure electronic data capture systems approved by the ethics committee.

Such platforms may be preferred for studies involving higher data sensitivity, longitudinal follow-up, or enhanced audit trail requirements.

6. Data Storage and Security

6.1 Storage Environment

- Data collected through electronic platforms will be stored on secure cloud-based or institutionally hosted servers.
- Where cloud services are used, configurations will, to the extent feasible, utilize **India-based data storage regions**.

6.2 Security Safeguards

- Encryption of data in transit and at rest;
- Password protection and role-based access controls;
- Access limited to authorized personnel located in India;
- Periodic review of access permissions.

Raw and identifiable datasets will not be shared outside India.

7. Anonymization and De-identification

- Anonymization and de-identification will be conducted locally in India prior to any data sharing.
- This will include removal of direct identifiers and appropriate treatment of indirect identifiers.
- Where linkage is required, re-identification keys will be stored separately, securely, and access-restricted.

Once anonymized, data will be reviewed to assess residual re-identification risk.

8. Data Processing and Analysis

- Initial data cleaning and processing will be undertaken within India.
- Only anonymized, aggregated, or derived datasets required for collaborative analysis will be prepared for sharing.
- Re-identification attempts are strictly prohibited.

9. Data Sharing with International Collaborators

- Data sharing will be limited to anonymized, processed datasets.
- Sharing will be governed by a formal **Data Sharing Agreement (Annexure 1)**.
- Data will be transferred using secure, encrypted channels.

This approach ensures compliance with Indian law while aligning with international best practices.

10. Data Retention and Archiving

- Data will be retained for periods approved by ethics committees and required by law.
- Archived data will remain encrypted and access-controlled.
- Data will be securely deleted or irreversibly anonymized at the end of the retention period.

11. Data Breach Management

- Suspected or confirmed data breaches will be investigated promptly.
- Notifications will be made to relevant authorities and ethics committees as required under Indian law.
- Corrective and preventive actions will be documented.

12. Review and Updates

This SOP will be reviewed periodically and updated to reflect changes in law, ethical guidance, or best practices.

Annexure 1: Data Sharing Agreement (DSA)

For International Collaborators

This Data Sharing Agreement (DSA) forms an annexure to the GRID Council SOP on Data Privacy, Confidentiality, and Data Sharing.

1. Parties

- **Data Custodian:** GRID Council, India
- **Data Recipient:** International Collaborating Institution / Investigator

2. Purpose

Data are shared solely for collaborative research purposes as defined in the approved study protocol and ethics approvals.

3. Nature of Data Shared

- Only anonymized, de-identified, and processed datasets will be shared.
- No direct identifiers, linkage keys, or raw datasets will be shared.

4. Legal and Ethical Basis

- Data sharing is governed by Indian law, including the DPDP Act, 2023.
- Shared datasets are anonymized and do not constitute transfer of personal data.
- Data handling by the recipient shall align with internationally accepted principles reflected in GDPR and HIPAA.

5. Recipient Obligations

The Data Recipient agrees to: - Use data only for approved purposes; - Implement appropriate security safeguards; - Restrict access to authorized personnel; - Not attempt re-identification or onward sharing.

6. Retention and Destruction

Data will be retained only for the duration necessary for the research and securely deleted thereafter.

7. Breach Notification

Any data breach involving shared data must be promptly reported to GRID Council.

8. Governing Law

This Agreement shall be governed by the laws of India.

9. Restrictions on Further Sharing

The Data Recipient shall not:- Share data with third parties without written consent- Use data for commercial purposes- Include data in public repositories without anonymization review

10. Publication and Attribution

- Joint publications require mutual agreement

- Acknowledgment of GRID Council and funding sources required

- Pre-publication review by GRID Council for data-related content

11. Dispute Resolution

Disputes shall be resolved through:

1. Good-faith negotiation

2. Mediation (if required)

3. Arbitration under Indian law

12. Acceptance

By receiving the data, the Data Recipient agrees to these terms.

For GRID Council
Name & Signature: ________________
Date: ____________

For International Collaborator
Name, Institution & Signature: ________________
Date: ____________