A Quick Guide to Data Management & Protection in Research

Proper data management is the backbone of ethical and credible research. It is more than just good practice—it is a critical component that builds trust with participants, ensures legal compliance, and upholds the integrity of your work. Mishandling data can cause real harm, destroy your credibility, and lead to significant legal and financial penalties for you and your institution.

What is Personally Identifiable Information (PII)?

Personally Identifiable Information (PII) is any data that can be used on its own or in combination with other information to identify, contact, or locate a single person.

Common examples of PII include:

- Names, ID numbers, passport details
- Phone numbers, email addresses, physical addresses
- Photographs, video recordings, audio voice recordings
- GPS coordinates and precise location data
- Biometric data (e.g., fingerprints, DNA)
- Financial account details

Important Note: Even "anonymized" data can sometimes be re-identified if combined with other datasets. Always treat research data with the utmost care.

Navigating Global Data Protection Laws

Most countries have established Data Protection Authorities (DPAs) that regulate how personal data is handled. Researchers must be aware of and comply with the laws in their country of operation.

Key regulations include:

- Europe: GDPR (General Data Protection Regulation) – Known for its strict rules and heavy fines.
- Kenya: Data Protection Act (2019)
- Tanzania: Personal Data Protection Act (2022)
- South Africa: POPIA (Protection of Personal Information Act, 2020)
- Nigeria: NDPR (Nigeria Data Protection Regulation, 2019)

- USA: HIPAA (for health data), plus various state laws like CCPA
- Brazil: LGPD (Lei Geral de Proteção de Dados)
- China: PIPL (Personal Information Protection Law)
- India: DPDP Act (Digital Personal Data Protection Act, 2023)

Bottom Line: Always check with your local regulatory body and secure the necessary licenses (e.g., as a data controller or processor) before you begin collecting any data.

Who is Authorized to Access Research Data?

Access to personal data must be strictly limited to:

1. Principal Investigator (PI): The primary custodian and responsible party.
2. Research Team Members: Only those who require access to perform their specific role.
3. IRBs & Regulators: May be granted limited or anonymized access for audit and oversight purposes.
4. Funders/Partners: Only if explicitly described in the participant consent form and governed by a formal Data Sharing Agreement.

Best Practices for Handling Data

Store Data Securely

- Encrypt digital files and use strong password protection.
- Lock physical documents in secure filing cabinets.
- Avoid storing data on personal devices or using unprotected USB drives.

Collect Minimally

- Adhere to the "minimum necessary" principle. Only collect data that is essential to your research objectives.

Manage Retention & Deletion

- Retain data only for the period required by your IRB (typically 5-7 years after study completion).
- Delete data securely: shred paper files and use certified digital file-wiping tools.

Share Data Responsibly

- Always obtain IRB approval before sharing any data.
- Whenever possible, share only anonymized or fully de-identified datasets.

- Use formal Data Sharing Agreements and secure transfer channels (never via personal email).

Consequences of Non-Compliance

Failing to protect participant data can have severe repercussions, including:

- Substantial financial fines and legal lawsuits.
- Suspension of research licenses for you or your institution.
- Loss of funding and irreversible damage to professional trust and reputation.
- Personal liability, as some laws hold individual researchers directly responsible for violations.

Quick Checklist for Researchers

- Register with your national data protection authority if required.
- Explain data use clearly in the consent process and read forms word-for-word.
- Collect only the minimum data necessary for your study.
- Store data securely, share it responsibly, and delete it properly.
- Include a detailed data management plan in every IRB application.

In short: Handle all research data like the valuable and sensitive asset it is—with security, legality, and profound respect for the participants who provided it.

At Global Research IRB (GRI), we provide expert support to help you navigate complex data protection laws, obtain the necessary licenses, and build robust, compliant data management systems that meet both global standards and local regulatory requirements.