



SOP-09 | Data Protection and Participant IDs

Standard Operating Procedure

Document	SOP-09
Status	Draft for internal approval
Version	0.1
Effective date	Upon approval
Owner	BEER Lab Manager
Review cycle	At least annually
Applies to	Projects and personnel within the scope of this SOP

Behavioral & Experimental Economics Research Lab · Tecnológico de Monterrey

1. Purpose

Protect participant information and ensure that identity, payment, recruitment, and analytical data are linked only when necessary and under controlled access.

2. Data classes

Class	Examples	Default handling
Direct identifiers	Name, email, phone, student ID	Separate, restricted, encrypted
Linking file	BEER ID ↔ study ID	Highly restricted, separate
Payment/admin	Bank reference, signature, amount paid	Separate from behavioral data
Research data	Choices, outcomes, survey responses	Project access controls
Sensitive data	Health, victimization, biometrics, precise location	Enhanced controls and minimum collection

3. Identifier architecture

The preferred architecture is ORSEE/contact ID → BEER participant ID → project experimental ID. Analytical files should use the project ID and should not contain direct identifiers unless scientifically necessary.

4. Access control

- Grant the minimum access needed for each role.
- Do not share accounts or credentials.
- Remove access promptly when staff leave a project.
- PI maintains an access list for files containing PII or sensitive data.

5. Storage and transfer

- Use institutionally approved or otherwise approved secure storage.
- Encrypt PII and sensitive data at rest and in transit when feasible.
- Do not transmit PII through personal messaging apps or unsecured email attachments.
- Field devices should use screen locks and encryption where supported.

6. Linking files

The file that connects direct identifiers to study IDs must be stored separately from research data and accessed only by staff who need re-identification for approved operational reasons.

7. Data minimization and retention

Collect only identifiers necessary for recruitment, follow-up, payment, or approved linkage. Delete or irreversibly de-identify PII when it is no longer needed, subject to consent, ethics requirements, legal retention obligations, and reproducibility needs.

8. Public or shared datasets

Before sharing data, assess re-identification risk, including combinations of indirect identifiers. Public release is never automatic merely because names have been removed.

9. Data breach

Suspected unauthorized access, lost devices containing research data, or accidental disclosure must be treated as an incident under SOP-10. Preserve logs and do not delete evidence needed to assess the breach.

10. Related documents

- SOP-02 Participant Pool and ORSEE
- SOP-08 Field Experiments
- SOP-10 Incident Reporting
- SOP-11 Project Closeout