SOP: Documentation and Secure Storage of Consent Forms

This SOP provides guidelines for the **documentation and secure storage of consent forms**, ensuring all consent forms are accurately completed, systematically recorded, and stored in a secure manner. It includes procedures for maintaining confidentiality, controlling access, and complying with relevant legal and regulatory requirements to protect sensitive information and uphold organizational accountability.

1. Purpose

To establish a standardized process for documenting, recording, and securely storing all consent forms collected within the organization, ensuring confidentiality and compliance with applicable laws.

2. Scope

This procedure applies to all staff responsible for obtaining, handling, and storing participant or client consent forms in both paper and electronic formats.

3. Responsibilities

- **Staff Obtaining Consent:** Ensure accurate completion of consent forms.
- **Data/Records Manager:** Oversee the secure storage and access to consent forms.
- **Supervisors:** Monitor adherence to this SOP and conduct periodic reviews.

4. Procedure

4.1 Documentation of Consent Forms

1. Verify participant understanding and willingness before obtaining consent.
2. Ensure all fields on the consent form are completed, including signatures and dates.
3. Give a copy of the signed form to the participant, if required.
4. Record the consent form in the consent log (manual or electronic), noting participant ID, date, and staff signature.

4.2 Secure Storage of Consent Forms

1. Store paper consent forms in locked cabinets located in restricted-access rooms.
2. Label files clearly with non-identifiable codes if possible.
3. Scan and store electronic copies in a password-protected, encrypted digital repository.
4. Back up electronic consent forms regularly following IT security policy.

4.3 Access Control

1. Limit access to consent forms to authorized personnel only.
2. Maintain an access log (manual or electronic) for persons viewing or handling consent forms.
3. Do not share or transmit consent forms via unsecured channels (e.g., email, personal drives).

4.4 Retention and Disposal

1. Retain consent forms for the period required by law or organizational policy (typically 5-10 years).
2. Securely shred paper forms and permanently delete electronic forms after retention period.
3. Document the date and method of disposal in the consent form log.

5. Confidentiality

- All staff must sign a confidentiality agreement and be trained on data protection protocols.
- Do not disclose consent information to unauthorized individuals.

6. Compliance and Review

- Comply with applicable legal, regulatory, and organizational requirements (e.g., GDPR, HIPAA).
- Review and update this SOP annually or when changes to processes occur.

7. Documentation

Document	Location	Retention
Signed Consent Forms	Locked Cabinet / Encrypted Server	5-10 years
Consent Form Log	Records Office / Secure Database	5-10 years
Access Logs	Records Office / Secure Database	5-10 years
Disposal Records	Records Office	Permanent

8. References

- Relevant organizational policies on data protection and confidentiality
- Applicable legal/regulatory requirements (e.g., GDPR, HIPAA)
- Industry best practices for records management

9. Revision History

Date	Version	Changes
2024-06-01	1.0	Initial version