

SOP: Data Review and Audit Trail Documentation

This SOP details the processes for **data review and audit trail documentation**, encompassing data verification, validation procedures, audit trail creation, and maintenance. It ensures accuracy, traceability, and compliance with regulatory standards by providing systematic guidelines for reviewing data entries, recording changes, and preserving audit trails to support transparency and accountability in data management.

1. Purpose

To define standardized procedures for data review, validation, and the documentation and maintenance of audit trails, ensuring data integrity and regulatory compliance.

2. Scope

This SOP applies to all personnel involved in data entry, review, and management processes within the organization, including electronic and paper-based records.

3. Responsibilities

- **Data Owners:** Ensure the accuracy and completeness of data entered.
- **Reviewers:** Perform data verification and validation.
- **IT/QA Personnel:** Maintain audit trail mechanisms and oversee compliance with this SOP.

4. Procedure

4.1 Data Review

1. Access data entries as required by the workflow.
2. Verify data for completeness, accuracy, and logical consistency.
3. Cross-check data with source documents, if applicable.
4. Flag any inconsistencies, errors, or omissions for correction.

4.2 Data Validation

1. Ensure data entries comply with predefined validation rules and formats.
2. Document validation checks performed and outcomes.
3. Forward validated data for further processing or archive as final record.

4.3 Audit Trail Documentation

1. For electronic systems, ensure audit trail functionality is enabled and configured to capture:
 - User identification (who performed the action)
 - Date and time stamp of actions
 - Description of action or change performed
 - Previous and new values (where applicable)
2. For manual records, log all corrections or changes with:
 - Initials/signature of the person making the change
 - Date and justification for the change

4.4 Maintenance of Audit Trails

1. Protect audit trail data from unauthorized modification or deletion.
2. Back up audit trails as part of regular data backup routines.
3. Retain audit trails according to organizational retention policies and regulatory requirements.
4. Review and monitor audit trails periodically to detect unusual or unauthorized activities.

5. Documentation

- Retain all data review, validation, and audit records in accordance with the data retention policy.
- Ensure availability of documentation for internal and external audits.

6. References

- Applicable regulatory guidelines (e.g., 21 CFR Part 11, GDPR, etc.)
- Organizational data integrity policies

7. Revision History

Version	Date	Description	Author
1.0	2024-06-20	Initial SOP creation.	[Author Name]