SOP-002 Record Control Procedure ## 1. Purpose

The purpose of this procedure is to define the controls for the identification, storage, security, integrity, retrieval, retention time, and disposition of records. This ensures that evidence of conformity to requirements and of the effective operation of the QMS is maintained in compliance with ISO 13485:2016 (Sec 4.2.5), MDR (EU) 2017/745, IVDR (EU) 2017/746, and 21 CFR Part 820.180. This procedure also ensures data integrity per 21 CFR Part 11.

2. Scope

This procedure applies to all Quality Records generated within the QMS.

- In Scope: Device History Records (DHR), Audit Reports, Training Logs, CAPA files, Management Review Minutes, Supplier Files, Validation Reports, Non-Conformity Reports.
- Out of Scope: Documents (SOPs, Templates) which are controlled under the *Document Control Procedure*.

3. Definitions

- Record: A document stating results achieved or providing evidence of activities performed. Records are immutable snapshots of history.
- ALCOA+: Data integrity framework requiring records to be Attributable, Legible, Contemporaneous, Original, and Accurate.
- DHR (Device History Record): A compilation of records containing the complete production history of a specific finished device (batch/lot).
- Retention Period: The specific duration of time a record must be kept before destruction is permitted.

4. Roles and Responsibilities

4.1 Record Creator / Owner

- Ensure data entered is accurate, complete, and truthful.
- Generate the record at the time the activity occurs (Contemporaneous).
- Lock/Sign the record upon completion.

4.2 Quality Assurance (QA)

- Define retention periods.
- Manage the archive and retrieval requests during audits.
- Authorize the destruction of records after the retention period expires.

4.3 IT / System Admin

- Ensure regular backups of the eQMS database.
- Ensure security controls prevent unauthorized deletion or modification of records.

5. Record Lifecycle Definitions

The eQMS manages records through the following states. Unlike documents, records do not have versions; they have entry stages.

Status	Definition	Access Rights
OPEN / IN-PROGRESS	Data is currently being entered. The record is not yet complete.	Edit: Creator. Read: Creator
LOCKED / PENDING APPROVAL	Data entry is finished. Record is locked and awaiting review/signature (if applicable).	Edit: None. Read: Reviewer, QA
COMPLETED / SIGNED	The record is final, signed, and acts as official evidence. It is strictly Read-Only.	Edit: None (Corrections require Audit Trail). Read: Authorized Users
ARCHIVED	The record is no longer active but is kept for the retention period.	Edit: None. Read: QA/Admin (Retrieval only)
DESTROYED	The record has been permanently deleted after the retention period (metadata log preserved).	Edit: None. Read: None

6. Procedure

6.1 Record Generation

1. Records must be generated using the current, approved version of the relevant Form or Template (controlled via SOP-001).
2. Records must be completed contemporaneously (at the time the work is performed). Backdating is strictly prohibited.
3. All mandatory fields in the electronic form must be filled. The system shall not allow submission if mandatory fields are empty.

6.2 Identification and Traceability

1. The eQMS automatically assigns a unique Record ID (e.g., `REC-2024-XXXX` or `NC-005`) upon creation.
2. Records must be traceable to:
   - The product (Batch/Serial Number).
   - The process (Equipment ID, Process ID).
   - The person (User ID).

6.3 Data Integrity and Corrections

1. Immutability: Once a record is status “COMPLETED”, the data fields cannot be overwritten.
2. Corrections (Electronic): If a correction is necessary after the record is locked:
   - The user must create a “Correction Entry” linked to the original record.
   - The system must capture: Who made the change, When (timestamp), Why (reason for change), and preserve the Old Value and New Value.
   - The original data must remain visible in the Audit Trail (it must not be obscured).

6.4 Electronic Signatures

1. Records requiring approval (e.g., Batch Release, Validation Report) must be signed electronically.
2. The signature signifies that the signer has reviewed the data and accepts responsibility for its accuracy.
3. Per 21 CFR Part 11, the signature is permanently linked to the record and cannot be excised.

6.5 Record Retention

1. General Rule: Records shall be retained for the lifetime of the medical device plus two (2) years, or as required by applicable regulations (e.g., 5 years minimum for MDR Annex IX), whichever is longer.
2. For this system, the default retention period is set to 15 Years (covering most device lifetimes) unless specified otherwise in a specific plan.

6.6 Storage and Retrieval

1. Electronic records are stored in the secure SQL database.
2. Records must remain legible and accessible throughout the retention period.
3. Backups: Database backups are performed daily to prevent loss of records.

6.7 Disposition / Destruction

1. Upon expiration of the retention period, the System Admin (with QA authorization) may purge records.
2. A "Certificate of Destruction" or a metadata log entry must be kept, indicating *which* records were destroyed and *when*.

7. Electronic System Requirements (Technical Specs for QA)

To ensure compliance, the Python/SQL system includes:

- INSERT-Only Logic: For critical data, the system prefers appending new rows over `UPDATE` operations to preserve history.
- Searchability: Records must be queryable by Date, User, Batch Number, or Record ID.
- Audit Trail: A separate SQL table `audit_log` records every transaction against the record tables. This log is read-only for all users.
- Data Validation: Input fields enforce data types (e.g., dates cannot be in the future for "Activity Date") to prevent errors at the source.