Standard Operating Procedure

Title: Data Management, Data Handling, Security, Confidentiality, and HIPAA Compliance
Study: Lionheart Klotho-Up Study
SOP No.: LKU-SOP-DM-002
Version: 1.0
Effective Date: March 7, 2026
Prepared By: Lionheart Health Study Operations
Approved By: Dr. Leslie Miller, Study Director
Review Cycle: Every 12 months or sooner if required by regulatory, operational, or systems changes

---

1. Purpose

This Standard Operating Procedure establishes the requirements for the proper collection, receipt, handling, entry, review, storage, transfer, protection, retention, and controlled use of study data for the Lionheart Klotho-Up Study.

This SOP is intended to ensure:

- data integrity, accuracy, consistency, and traceability;
- appropriate handling of source data and study databases;
- protection of subject confidentiality and privacy;
- compliance with applicable data protection standards, including **HIPAA** requirements where applicable;
- secure handling of protected health information and personally identifiable information;
- proper role-based access to study data;
- readiness for monitoring, audit, DSMB review, and regulatory inspection.

This SOP is separate from, but coordinated with:

- the Baseline and 1-Year Follow-Up Data Collection SOP;
- the Adverse Event Reporting SOP;
- applicable Quality Systems procedures;
- any study-specific Data Management Plan.

---

2. Scope

This SOP applies to all personnel, systems, consultants, vendors, sites, and affiliated study team members who create, receive, access, review, analyze, transmit, or store study data related to the Lionheart Klotho-Up Study.

This includes:

- paper records;
- electronic records;
- spreadsheets;
- case report forms;
- source documents;
- laboratory reports;
- imaging results;
- biomarker reports;
- subject questionnaires;
- safety records;
- statistical datasets;
- de-identified and coded data extracts;
- data shared with monitors, auditors, DSMB members, statisticians, or regulatory consultants.

---

3. Related Documents

This SOP should be read together with:

- Study Protocol
- Investigator's Brochure
- Informed Consent Form and HIPAA Authorization, where applicable
- Data Management Plan
- Monitoring Plan
- Adverse Event Reporting SOP
- DSMB Charter
- Source Documentation Guidelines
- Record Retention Policy
- Information Security Policy
- Password / Access Control Policy
- Vendor Oversight Procedures
- Quality Management / CAPA Procedures

---

4. Definitions

Protected Health Information (PHI):
Individually identifiable health information protected under HIPAA.

Personally Identifiable Information (PII):
Information that can identify an individual directly or indirectly.

Source Data:
Original records in which study information is first documented.

eCRF / CRF:
Electronic or paper case report form used to capture protocol-required study data.

Coded Data:
Data labeled with a unique study ID instead of direct identifiers.

De-identified Data:
Data stripped of identifiers to the extent required for the intended use and applicable law.

Minimum Necessary Standard:
The HIPAA principle that access, use, and disclosure of PHI should be limited to the minimum necessary to accomplish the intended purpose, unless an exception applies.

Audit Trail:
A secure, time-stamped record showing creation, modification, deletion, or review of data.

Data Query:
A documented request for clarification or correction of incomplete, inconsistent, or implausible data.

---

5. Roles and Responsibilities

5.1 Dr. Leslie Miller, Study Director

Dr. Leslie Miller provides overall study oversight regarding the appropriate medical and scientific use of study data, including:

- oversight of medically relevant data review;
- review of significant data irregularities affecting study interpretation;
- support of safety-related data review and escalation.

5.2 Sejal Chaudhari, Senior Research Coordinator

Sejal Chaudhari is responsible for operational oversight of study data management activities, including:

- supervision of study data workflows;
- oversight of data collection completeness and consistency;
- management of unresolved data issues;
- coordination with regulatory and quality personnel on data-related concerns;
- confirmation that study personnel are trained on applicable procedures.

5.3 Suhani Khandelwal, Research Coordinator / Biostatistician

Suhani Khandelwal is responsible for day-to-day data handling and dataset support activities, including:

- maintaining study data tracking tools;
- organizing baseline and follow-up data packages;
- supporting data cleaning and reconciliation;
- reviewing datasets for missingness, outliers, and logical inconsistencies;
- preparing internal data summaries and status reports;
- escalating data integrity or confidentiality concerns immediately to Sejal Chaudhari.

5.4 Larry Stevens, Chief Regulatory Consultant

Larry Stevens provides oversight and guidance on:

- regulatory adequacy of data documentation;
- records needed for inspection readiness;
- reporting implications of data discrepancies, deviations, or safety-related findings;
- alignment of data handling practices with applicable requirements.

5.5 Ben Boytor, Chief Quality Systems Consultant

Ben Boytor provides quality systems oversight, including:

- data process control review;
- audit readiness guidance;
- corrective and preventive action support;
- review of recurring documentation and system failures;
- oversight of SOP adherence from a quality systems perspective.

5.6 Site Personnel and Authorized Vendors

Site staff and authorized vendors are responsible for:

- timely and accurate documentation;
- secure handling of records;

- maintaining confidentiality;
- responding to data clarification requests;
- complying with approved study procedures and applicable privacy requirements.

---

6. General Principles

All study data must be managed according to the following principles:

- accuracy;
- completeness;
- consistency;
- legibility;
- traceability;
- confidentiality;
- security;
- controlled access;
- auditability;
- timely correction of discrepancies.

All personnel must use study data only for authorized study purposes and only to the extent necessary for their assigned role.

---

7. Data Categories Covered

The following data categories are covered by this SOP:

- subject identifiers and enrollment logs;
- informed consent and HIPAA authorization records;
- demographics and medical history;
- concomitant medications and interventions;
- laboratory and biomarker reports;
- imaging and functional test reports;
- questionnaires and subject-reported outcomes;
- safety event data;
- protocol deviation documentation;
- monitoring and audit records;
- statistical analysis datasets;
- DSMB summary materials;
- publication support datasets;
- archived study data and backups.

8. Procedure

8.1 Data Collection Standards

1. Data must be recorded promptly in source documents or approved systems.
2. All entries must be attributable to the individual making the entry.
3. Study records must be accurate, legible, contemporaneous, and complete.
4. No study data may be fabricated, backdated, altered inappropriately, or entered without supporting documentation.
5. When corrections are necessary, the original entry must remain reconstructable through an audit trail or dated correction process.

8.2 Subject Identification and Coding

1. Each participant shall be assigned a unique study identifier.
2. Direct identifiers shall be separated from study analysis datasets whenever feasible.
3. Subject identification logs linking identifiers to study IDs shall be stored securely and accessed only by authorized personnel.
4. Routine data review, summary reporting, and statistical analysis should use coded subject identifiers rather than direct identifiers whenever possible.

8.3 Receipt and Logging of Data

Upon receipt of study data from sites, labs, vendors, or coordinators:

1. the receipt date shall be documented where appropriate;
2. the document or file shall be associated with the correct subject and visit;
3. completeness and readability shall be checked;
4. unexpected or mismatched records shall be flagged and investigated;
5. any missing critical elements shall be documented and followed up.

Suhani Khandelwal shall maintain study data tracking logs and completeness logs under the supervision of **Sejal Chaudhari**.

8.4 Data Entry and Reconciliation

1. Data entry shall occur only in approved study forms, logs, or systems.
2. Critical fields shall be reviewed for consistency with source documentation.
3. Data discrepancies shall be documented through formal queries or discrepancy notes.
4. Query resolution must be traceable and, where appropriate, dated and attributable.
5. Updated values must reflect verified information from source documentation or documented clarification.

Examples of critical fields include:

- subject ID
- consent date
- eligibility status
- visit date
- primary endpoint values
- serious adverse event information
- discontinuation date and reason
- death, hospitalization, or medically significant events

8.5 Data Quality Review

Routine data quality review shall include:

- missing field checks;
- date consistency checks;
- logic checks;
- range checks where applicable;
- duplicate record review;
- source-to-CRF comparison for critical data elements;
- review of outliers and unusual patterns;
- review of protocol window compliance for major visits.

Suhani Khandelwal shall support first-line review.
Sejal Chaudhari shall oversee second-line operational review.
Ben Boytor may review systemic quality concerns.
Larry Stevens shall be consulted when data issues may have regulatory implications.

8.6 Data Security and System Controls

All electronic study data must be maintained in secure systems or controlled storage environments with reasonable safeguards, including as applicable:

- unique user credentials;
- password protection;
- role-based access controls;
- encrypted storage or secure hosted platforms where appropriate;
- restricted download and sharing permissions;
- automatic or manual audit trails;
- backup and recovery procedures;
- secure file transfer methods;
- protection against unauthorized alteration or deletion.

Shared drives, cloud folders, laptops, and portable media containing study data must be secured and limited to authorized users.

No study data containing PHI should be stored on unsecured personal devices or transmitted through unapproved insecure channels.

8.7 Paper Record Handling

Paper records containing study data or PHI must be:

- stored in locked cabinets, locked rooms, or controlled-access areas;
- protected from unauthorized access, loss, or damage;
- organized to preserve traceability and retrieval;
- transported only when necessary and in a secure manner.

Printing of PHI-containing records should be limited to operational necessity.

8.8 HIPAA Compliance Requirements

Where HIPAA applies, the study team shall comply with applicable HIPAA privacy and security requirements.

This includes:

1. using or disclosing PHI only as permitted by signed authorization, protocol requirements, IRB approval, business associate arrangements, applicable law, or other permitted basis;
2. limiting access to PHI to the **minimum necessary** for the role and task;
3. restricting use of direct identifiers in data summaries whenever not required;
4. safeguarding PHI from unauthorized access, disclosure, alteration, or loss;
5. ensuring that personnel handling PHI are trained on privacy and confidentiality obligations;

6. documenting and escalating any suspected privacy incident, breach, or unauthorized disclosure immediately.

Where a separate HIPAA Authorization is used, study staff shall confirm that authorization is present before use or disclosure of PHI beyond what is otherwise permitted.

8.9 Confidentiality and Minimum Necessary Access

Access to subject-level identifiable data shall be limited to personnel with a legitimate study need.

Examples:

- coordinators may access subject contact and scheduling information as needed;
- statisticians should generally use coded datasets unless direct identifiers are necessary;
- quality and regulatory reviewers may access records necessary for oversight;
- DSMB materials should be prepared in appropriately limited form whenever possible.

All personnel must avoid discussing subject-identifiable information in public, unsecured, or non-authorized settings.

8.10 Data Transfer and Sharing

When transferring study data:

1. only authorized recipients may receive the data;
2. the data shared must be limited to the minimum necessary for the intended purpose;
3. secure transfer methods shall be used;
4. transfer of identifiable data shall be documented where appropriate;
5. de-identified or coded data should be used in preference to direct identifiers whenever possible.

Data sharing with monitors, auditors, statisticians, consultants, DSMB members, or publication partners must follow approved study governance and confidentiality controls.

8.11 Safety Data Handling

Safety-related data must be handled with particular urgency and care.

If data review reveals a possible adverse event, serious adverse event, unanticipated problem, or medically significant abnormality:

- the issue must be escalated immediately to **Sejal Chaudhari** and the appropriate medical oversight pathway;
- all handling must follow the separate **Adverse Event Reporting SOP**;
- safety data must remain traceable from source through reporting records.

This SOP does not replace the Adverse Event Reporting SOP.

8.12 Data Corrections and Change Control

When correcting study data:

1. the change must be attributable;
2. the reason for change should be documented where required;
3. original information must remain reconstructable;
4. corrections must not obscure the original entry;
5. significant repeated errors may require retraining or CAPA review.

Systemic data issues shall be reviewed by **Ben Boytor** and, when needed, by **Larry Stevens** and **Dr. Leslie Miller**.

8.13 Backups, Retention, and Archiving

Study data must be retained according to:

- protocol requirements;
- sponsor requirements;
- IRB requirements;
- applicable legal and regulatory retention requirements.

Electronic data should be backed up according to the applicable system or organizational policy.

Archived study records must remain:

- retrievable;
- legible;
- protected from unauthorized access;
- preserved in a manner that supports audit and inspection readiness.

8.14 Privacy Incidents, Breaches, and Unauthorized Disclosures

Any suspected or confirmed:

- privacy incident,
- unauthorized disclosure,
- lost device containing study data,
- misdirected email or file,
- improper access,
- data corruption,
- security compromise

must be reported immediately to:

- **Sejal Chaudhari**
- **Larry Stevens**
- **Ben Boytor**
  and escalated further according to applicable organizational privacy, regulatory, and quality procedures.

Where medically relevant or operationally significant, **Dr. Leslie Miller** shall also be informed.

Documentation of incident assessment, containment, corrective actions, and notifications shall be maintained as required.

8.15 Audit Trails and Inspection Readiness

Study data systems and records must support reconstruction of:

- who entered or changed data,
- what was changed,
- when it was changed,
- why it was changed where applicable,
- how final analyzed data trace back to original records.

Data files, logs, and documentation should be maintained in a manner that supports sponsor review, monitoring, audit, DSMB review, and regulatory inspection.

8.16 Training

All personnel with access to study data must be trained, as appropriate, on:

- this SOP;
- confidentiality requirements;
- HIPAA requirements where applicable;
- secure data handling practices;
- password and access control expectations;
- procedures for reporting privacy or data integrity incidents.

Training must be documented before personnel independently perform covered tasks.

---

9. Escalation Pathway

Data completeness or discrepancy issue
Suhani Khandelwal → Sejal Chaudhari

Clinical significance or medically important data issue
Sejal Chaudhari → Dr. Leslie Miller

Regulatory documentation or reportability issue
Sejal Chaudhari → Larry Stevens

Quality systems, recurring process failure, CAPA issue
Sejal Chaudhari → Ben Boytor

Privacy incident / HIPAA concern / unauthorized disclosure
Immediate escalation to Sejal Chaudhari, Larry Stevens, and Ben Boytor, with further escalation per applicable policy

Adverse event or possible safety signal
Immediate handling per Adverse Event Reporting SOP

---

10. Compliance

Failure to comply with this SOP may compromise:

- subject privacy;
- HIPAA compliance;
- data integrity;

- study validity;
- regulatory readiness;
- sponsor and site credibility.

Noncompliance may result in retraining, corrective action, preventive action, restricted access, or other remedial measures.

---

11. SOP Summary Statement

For the Lionheart Klotho-Up Study, all study data must be collected, handled, reviewed, stored, transferred, and retained in a secure, traceable, and confidential manner. **Suhani Khandelwal, Research Coordinator / Biostatistician**, under the supervision of **Sejal Chaudhari, Senior Research Coordinator**, shall support day-to-day data management and data quality activities. **Dr. Leslie Miller** provides medical and scientific oversight, **Larry Stevens** provides regulatory oversight, and **Ben Boytor** provides quality systems oversight. All personnel shall protect subject confidentiality and comply with applicable **HIPAA** privacy and security requirements where applicable. This SOP is linked to the study's safety governance and must be followed together with the separate Adverse Event Reporting SOP.

---

12. Signature Block

Prepared by:

Name:
Title:
Date:

Reviewed by:

Sejal Chaudhari
Senior Research Coordinator
Date:

Larry Stevens
Chief Regulatory Consultant
Date:

Ben Boytor
Chief Quality Systems Consultant
Date:

Approved by:

Dr. Leslie Miller
Study Director
Date:

Cross-Reference Statement for Prior SOP

This SOP shall be read together with LKU-SOP-DC-001, Baseline and 1-Year Follow-Up Data Collection, Review, Quality Control, and Safety Oversight. All study personnel responsible for collecting or reviewing subject data must comply with both SOPs. Where data privacy, security, confidentiality, or HIPAA handling requirements apply, LKU-SOP-DM-002 shall control. Where adverse event identification or reporting is involved, the Adverse Event Reporting SOP shall control.

\