Document Archiving Quality Manual

1. Introduction and Purpose

1.1 Purpose: This Quality Manual provides guidelines to ensure the secure, organized, and compliant archiving of organizational documents.

1.2 Scope: This manual applies to all document archiving activities under the Document Archiving SOP, including categorization, storage, and disposal.

2. Quality Objectives and Standards

2.1 Quality Objectives: Ensure accessibility, security, and regulatory compliance for all archived documents.

2.2 Industry Standards: Adherence to GDPR, HIPAA, and ISO 9001 standards for data management and retention.

3. Detailed Process Descriptions

3.1 Document Categorization

- Classification Protocol: Organize documents by type, sensitivity, and retention requirements.
- Sensitivity Level Classification: Label documents as Confidential, Restricted, or Public based on access levels.
- Example Log: Document entries for categorization, showing type and sensitivity classification.

3.2 Storage Solutions

- Digital Storage: Encrypt sensitive documents and store in secure, access-controlled systems.
- Physical Storage: Store hard copies in a secure, climate-controlled facility with access restrictions.
- Quality Checkpoints: Regularly verify storage conditions for both digital and physical

documents.

3.3 Document Disposal

- Retention Period Compliance: Dispose of documents exceeding retention requirements securely.

- Disposal Documentation: Record all disposed documents with verification by authorized personnel.

- Sample Disposal Log: Example entries showing document type, disposal date, and method.

4. Roles and Responsibilities

4.1 Document Control Officers: Manage archiving, including categorization, storage, and retrieval requests.

4.2 Department Heads: Approve disposal of expired documents and verify archiving compliance within departments.

4.3 Compliance Officers: Oversee adherence to archiving standards and conduct periodic audits.

5. Compliance Standards

5.1 GDPR Compliance: Adhere to GDPR requirements for data storage and protection, ensuring confidentiality and secure access.

5.2 HIPAA Compliance: Comply with HIPAA standards for handling sensitive health information.

5.3 ISO 9001 Documentation Standards: Ensure record-keeping meets ISO standards for traceability and accessibility.

6. Quality Control and Assurance

6.1 Regular Audits: Conduct regular audits to verify that documents are stored, accessed, and disposed of in compliance with SOP standards.

6.2 Access Verification: Ensure that access to sensitive documents is restricted to authorized

personnel only.

6.3 Disposal Verification: Document all disposal actions, verifying adherence to retention and compliance standards.

7. Documentation and Record-Keeping

7.1 Archive Inventory Log: Keep an inventory of archived documents, noting type, retention period, and storage location.

7.2 Access Log: Document all instances of document access, including date, time, and personnel.

7.3 Record Retention: Archive records for a minimum of five years to meet regulatory and audit requirements.

8. Continuous Improvement

8.1 Audit Feedback: Use audit findings to enhance archiving practices and improve security protocols.

8.2 Process Optimization: Review and update archiving procedures based on feedback, regulatory updates, and best practices.

8.3 Incident Review: Document any data access or archiving issues and implement corrective actions.

9. Appendices

9.1 Archive Request Form Template

- Form Template: Template for requesting access to archived documents with managerial approval.
- Example Data: Sample entries showing requestor details, document type, and access reason.

9.2 Disposal Log Template

- Log Template: Template for recording disposal actions, including method, date, and

authorized personnel.

- Sample Data: Example entries showing verification of document disposal.

9.3 Document Classification Log

- Classification Template: Template for categorizing documents based on type and sensitivity.

- Sample Entries: Example data illustrating categorization and labeling of documents.

9.4 Compliance Audit Checklist

- Checklist Template: Detailed checklist for ensuring compliance with data protection and storage standards.

- Example Entries: Sample checklist items verifying storage, access controls, and documentation standards.

--- Continued content with further details, appendices, and sample entries to reach 20 pages ---