Standard Operating Procedure (SOP)
Health Records Retention and Archiving Policies

SOP Number: HRR-001
Effective Date: [Insert Date]
Review Date: [Insert Date]
Version: 1.0
Author: [Name/Department]

1. Purpose

This SOP details the **health records retention and archiving policies**, including guidelines for the secure storage, duration, and systematic disposal of health-related documents. It emphasizes compliance with legal and regulatory requirements, confidentiality and privacy protections, secure digital and physical archiving methods, access control, and procedures for efficient retrieval and destruction of records. The purpose is to maintain accurate, accessible, and protected health records to support patient care, auditing, and legal obligations while safeguarding sensitive information.

2. Scope

This SOP applies to all health-related records maintained by the organization, in both paper and electronic formats, and to all staff responsible for the management, storage, access, retention, retrieval, and destruction of such records.

3. Definitions

- **Health Records:** Any documentation (physical or electronic) related to patient care, including medical histories, diagnoses, treatment records, and test results.
- **Retention Period:** The mandated duration for keeping a record before eligible for destruction.
- **Archiving:** Transfer of inactive records to a secure storage system for long-term retention.
- **Destruction:** Secure and permanent deletion or disposal of records at end of retention period.
- **Confidentiality:** Protection of patient and health information from unauthorized access.

4. Responsibilities

- **Health Information Management (HIM) Department:** Oversees implementation and compliance with retention and archiving policies.
- **IT Department:** Manages secure digital storage and record destruction for electronic records.
- **All Staff:** Ensures records are handled, stored, and disposed of per policy guidelines.
- **Compliance Officer:** Monitors regulatory changes and updates SOP as required.

5. Policy

1. **Retention Schedule:**
    - Health records must be retained in accordance with federal, state, and local regulations (see Schedule Table below).
2. **Storage & Archiving:**
    - Physical records must be stored in secure, access-restricted areas protected from fire, flood, theft, and unauthorized access.
    - Electronic records must be stored on encrypted, access-controlled servers with regular backups and robust cybersecurity measures.
3. **Access Control:**
    - Only authorized personnel may access health records. Access levels are defined based on job role and necessity.
4. **Retrieval:**
    - Archived records must be indexed and retrievable within the timeframe required for patient care or legal inquiries.
5. **Disposal/Destruction:**

- At the end of the retention period, records must be destroyed securely (e.g., shredding, incineration, permanent digital deletion) with appropriate documentation of destruction.

6. **Confidentiality and Compliance:**
   - All procedures must comply with relevant privacy regulations (e.g., HIPAA, GDPR).

6. Retention Schedule

Record Type	Minimum Retention Period	Disposal Method
Adult Medical Records	7 years after last date of service	Shred (paper), Secure delete (electronic)
Pediatric Medical Records	Age of majority + 7 years	Shred (paper), Secure delete (electronic)
Deceased Patient Records	5 years after death or as required by law	Shred (paper), Secure delete (electronic)
Regulatory/Audit Records	10 years or per regulation	Shred (paper), Secure delete (electronic)
Financial/Billing Records	7 years	Shred (paper), Secure delete (electronic)
Other (specify)	[As per policy/regulation]	As above

**Note: Retention periods may be extended in case of ongoing litigation, audits, or as mandated by law.*

7. Procedure

1. Classify, label, and file records (paper/electronic) upon creation or receipt.
2. Update retention and destruction date for each record type using the approved schedule.
3. Transfer inactive records promptly to secure archive systems, maintaining accessibility for authorized users.
4. Conduct periodic audits to confirm compliance, integrity, and accuracy of stored records.
5. At the end of the retention period, securely destroy records and keep documentation of the destruction (log date, method, responsible staff).
6. Report any breaches or unauthorized access in accordance with incident response protocols.

8. Confidentiality and Security

- Maintain strict access controls and confidentiality agreements for all personnel handling health records.
- Ensure robust physical and digital security measures are in place and periodically reviewed.
- Comply with all relevant information privacy laws and organizational policies.

9. References

- HIPAA Privacy Rule
- GDPR (if applicable)
- [Other relevant local/state/federal laws]
- Organizational information governance policy

10. Revision History

Version	Date	Summary of Changes	Approved By
1.0	[Insert Date]	Initial Release	[Name/Position]