Standard Operating Procedure (SOP): Disposal and Destruction of Confidential Patient Information

This SOP details the standardized procedures for the **disposal and destruction of confidential patient information**, ensuring compliance with legal, ethical, and organizational privacy requirements. It encompasses the identification of sensitive documents, secure handling practices, approved destruction methods such as shredding and incineration, documentation of destruction activities, staff training responsibilities, and protocols to prevent unauthorized access. The goal is to protect patient privacy, maintain data security, and mitigate risks associated with information breaches.

1. Purpose

To establish a consistent process for the secure disposal and destruction of confidential patient information to ensure compliance with HIPAA, relevant data privacy laws, and organizational policy.

2. Scope

This SOP applies to all employees, contractors, and volunteers who handle or manage confidential patient information in both physical (paper) and electronic formats.

3. Definitions

- **Confidential patient information:** Any information that can identify a patient, including but not limited to medical records, billing records, and personal identifiers.
- **Destruction:** The process of rendering information irretrievable and unusable.
- **Disposal:** The process of discarding information after adequate destruction.

4. Responsibilities

- **Department Managers:** Ensure staff compliance and that destruction is completed according to policy.
- **Staff:** Follow all procedures and report any breaches or concerns promptly.
- **IT and Records Teams:** Oversee destruction of electronic files and maintain destruction logs.

5. Procedure

1. **Identification of Sensitive Information:**
    - Regularly review documents/files to determine retention status.
    - Label and segregate items designated for destruction.
2. **Secure Handling Prior to Destruction:**
    - Store items awaiting destruction in a locked container or secure area.
    - Limit access only to authorized personnel.
3. **Approved Destruction Methods:**
    - **Paper records:** Use cross-cut shredders or certified destruction vendors; incineration for high-security documents if available.
    - **Electronic media:** Use data wiping software, degaussing, or physical destruction (e.g., crushing, shredding).
4. **Documentation:**
    - Complete a **Destruction Log** (see Table 1) including date, description, amount/type of materials, destruction method, and responsible staff.
5. **Review and Audit:**
    - Periodically audit destruction records for compliance.

6. Training

All staff will receive training on these procedures at onboarding and annually thereafter. Training records shall be maintained.

7. Breach Prevention and Reporting

- Access to confidential information must be restricted to authorized personnel only at all stages.
- All suspected or actual breaches must be reported immediately following organizational incident response

protocol.

8. Documentation

Table 1: Destruction Log Template

Date	Description of Records	Quantity/Type	Destruction Method	Person Responsible	Witness (if required)
YYYY-MM-DD	e.g., 2015 Discharge Summaries	2 boxes (paper)	Shredding	Jane Doe	John Smith

9. Review

This SOP will be reviewed annually or upon significant policy or regulatory changes.