SOP: Policies for Employee Termination and PHI Access Revocation

This SOP details **policies for employee termination and PHI access revocation**, outlining the procedures for managing employee departures, ensuring timely revocation of Protected Health Information (PHI) access, securing organizational data, and maintaining compliance with privacy regulations. It covers notification requirements, system access deactivation, return of company property, documentation protocols, and safeguarding sensitive patient information during the termination process to prevent unauthorized data access.

1. Purpose

To ensure consistent, prompt, and compliant handling of employee terminations and PHI access revocation to protect sensitive information and organizational assets.

2. Scope

This SOP applies to all employees, contractors, and temporary staff with access to PHI or any organizational systems containing sensitive information.

3. Definitions

- **PHI (Protected Health Information):** Any information, including demographic data, that relates to the individual's past, present, or future physical or mental health, the provision of health care, or payment for health care services.
- **Termination:** The end of employment or contractual relationship, whether voluntary or involuntary.
- **Access Revocation:** The process of disabling an individual's ability to use organizational systems and data, especially those containing PHI.

4. Roles and Responsibilities

Role	Responsibility
HR Department	Notify IT & Compliance, coordinate exit interviews, ensure proper documentation.
IT Department	Deactivate system and application access, collect company devices, delete/reassign emails.
Compliance Officer	Confirm PHI access is revoked, document actions for audit, oversee policy adherence.
Supervisor/Manager	Inform HR of impending termination, collect physical keys/badges, ensure property return.

5. Termination & PHI Access Revocation Procedure

1. **Notification:**
    - Manager notifies HR and Compliance at least two business days before termination, if possible.
2. **Pre-Termination Preparation:**
    - Identify all PHI and confidential system accesses.
    - HR schedules exit interview and property collection.
3. **Day of Termination:**
    - IT disables all system, application, and remote access immediately at the end of the employee's last working day.
    - Deactivate accounts on EHR/EMR, email, file storage, VPN, and physical access systems.
    - Collect all company property (badge, keys, laptop, phone, documents).
4. **Post-Termination Actions:**
    - Audit all account deactivations and remove or reassign PHI-related emails or files.
    - Compliance confirms and documents PHI access has been revoked.
    - Retain signed acknowledgement of property return and termination documents.
5. **Incident Handling:**
    - Any suspected or actual unauthorized access to PHI post-termination should be reported and investigated immediately following breach response policy.

6. Documentation & Recordkeeping

- Maintain records of termination, access revocation, and property return in personnel files for at least six years.
- Ensure all documentation is accessible for audits and regulatory review.

7. Compliance

- All activities must comply with HIPAA and other applicable privacy and security regulations.
- Periodic audits will assess adherence to this policy.

8. Review & Revision

- This SOP will be reviewed annually, or as needed following regulatory or organizational changes.

Document Owner: [Insert Responsible Department]
Effective Date: [Insert Date]
Version: 1.0
Next Review: [Insert Date]