Standard Operating Procedure (SOP): Protected Health Information (PHI) Storage and Encryption Standards

This SOP defines the **Protected Health Information (PHI) storage and encryption standards**, outlining secure methods for storing, accessing, and transmitting PHI. It covers data encryption protocols, access controls, compliance with HIPAA regulations, secure data backup and recovery, and guidelines for preventing unauthorized access or data breaches. The purpose is to protect patient confidentiality and ensure the integrity and security of sensitive health information.

1. Purpose

To establish standards for the secure storage, encryption, access, backup, and transmission of PHI in compliance with HIPAA and related regulations, ensuring patient data confidentiality and protection from unauthorized access or breaches.

2. Scope

This SOP applies to all workforce members, contractors, and vendors who store, process, or transmit PHI on behalf of the organization, regardless of location or device type.

3. Definitions

- **PHI:** Protected Health Information as defined under HIPAA.
- **Encryption:** The process of encoding data so only authorized parties can access it.
- **De-identification:** Removal of information that identifies an individual.

4. Responsibilities

- All staff must comply with PHI security standards.
- IT department is responsible for implementing and maintaining secure storage and encryption systems.
- Supervisors must ensure their team members complete related training.

5. Procedure

5.1 Storage of PHI

- All electronic PHI (ePHI) must be stored on encrypted devices or secure servers.
- Physical PHI must be stored in locked cabinets in restricted access areas.
- Cloud-based storage must comply with HIPAA and be approved by IT and Compliance departments.

5.2 Encryption Standards

- Data at rest: Must be encrypted using at least AES-256 or equivalent.
- Data in transit: Must utilize secure protocols (TLS 1.2 or higher) for all network transmissions containing PHI.
- Encryption keys must be stored and managed securely, separate from the encrypted data.

5.3 Access Controls

- Role-based access controls (RBAC) must be implemented to restrict PHI access to authorized users only.
- Multi-factor authentication (MFA) is required for all systems containing ePHI.
- Access logs must be maintained and reviewed regularly for unauthorized activity.

5.4 Backup and Recovery

- Regular encrypted backups of PHI must be performed and stored securely offsite.
- Backup media must be encrypted and access-controlled.
- Test restoration procedures quarterly to ensure backup viability.

5.5 Transmission of PHI

- Transmit PHI only via encrypted email, secure FTP, or organization-approved secure messaging systems.
- Never send PHI over unsecured channels, such as standard email or texting apps.

5.6 Prevention of Unauthorized Access/Breach

- Staff must report suspected data breaches immediately to IT/security personnel.
- Regularly train users on PHI security and privacy practices.
- Perform periodic security risk assessments and remediate identified vulnerabilities.

6. Compliance and Review

- This SOP will be reviewed annually or as needed to align with regulatory requirements and emerging best practices.
- All practices must comply with HIPAA, HITECH, and state-specific health information security regulations.

7. References

- Health Insurance Portability and Accountability Act (HIPAA)
- HITECH Act
- NIST SP 800-111, 800-52, 800-88
- Organizational Information Security Policy