SOP: Electronic Health Records (EHR) Security Measures

This SOP establishes **Electronic Health Records (EHR) security measures** to protect patient information confidentiality, integrity, and availability. It covers access control protocols, encryption standards, user authentication procedures, data backup and recovery processes, audit trail requirements, and compliance with relevant regulations such as HIPAA. The objective is to safeguard sensitive health data from unauthorized access, breaches, and cyber threats while ensuring seamless accessibility for authorized healthcare professionals.

1. Purpose

To define and standardize security practices for the management and protection of Electronic Health Records (EHR).

2. Scope

This SOP applies to all healthcare staff, IT personnel, contractors, and any individuals or systems accessing EHR within the organization.

3. Definitions

- **EHR:** Electronic Health Record, a digital version of a patient's paper chart.
- **PHI:** Protected Health Information.
- **HIPAA:** Health Insurance Portability and Accountability Act.

4. Access Control Protocols

1. Assign unique user IDs to all system users.
2. Establish user roles and permissions based on job requirements ("need to know").
3. Review user access levels quarterly and update as necessary.
4. Terminate access immediately upon staff separation or role change.

5. Encryption Standards

1. Encrypt EHR data at rest and in transit using industry-standard protocols (e.g., AES-256, TLS 1.2+).
2. Store encryption keys securely with access limited to authorized IT personnel.

6. User Authentication Procedures

1. Implement multi-factor authentication (MFA) for all EHR system logins.
2. Require strong passwords: minimum 8 characters, including letters, numbers, and symbols.
3. Enforce password changes every 90 days.
4. Monitor and restrict failed login attempts (lockout after 5 failures).

7. Data Backup and Recovery

1. Schedule automated, encrypted EHR backups at least daily.
2. Store backups both onsite and offsite (cloud or secure physical location).
3. Test backup restoration procedures quarterly.

8. Audit Trail Requirements

1. Enable logging of all EHR access, changes, and administrative actions.
2. Retain audit logs for a minimum of 6 years (per HIPAA).
3. Review audit trails monthly for suspicious activity.

9. Compliance and Training

1. Comply with HIPAA, HITECH, and applicable state/federal regulations.
2. Provide annual security awareness and EHR privacy training for all users.

10. Incident Response

1. Report suspected EHR breaches immediately to the Compliance Officer and IT Security.
2. Activate incident response procedures as per organization policy.
3. Document all incidents and notify affected parties as required by law.

11. Review and Revision

1. Review this SOP annually or upon regulatory/policy change.
2. Update and distribute revisions to all relevant personnel.

12. Approval

Prepared by	Title	Date
Approved by	**Title**	**Date**