# SOP: Electronic Health Records (EHR) Entry and Backup Process

This SOP details the **Electronic Health Records (EHR) entry and backup process**, encompassing accurate and timely data entry protocols, verification and validation of patient information, routine data backups, secure storage of electronic records, and procedures for data recovery in case of system failures. The aim is to maintain the integrity, confidentiality, and availability of patient health information to support quality healthcare delivery and compliance with regulatory requirements.

## 1. Purpose

To establish standardized procedures for the entry, validation, backup, and recovery of Electronic Health Records (EHR) to ensure accuracy, security, and compliance with legal and organizational requirements.

## 2. Scope

This SOP applies to all personnel involved in the management, entry, and maintenance of EHR within the organization.

## 3. Responsibilities

| Role | Responsibilities |
|---|---|
| Healthcare Providers | Ensure timely and accurate entry of patient data into the EHR system; verify the completeness of entered data. |
| Health Information Technicians | Validate data accuracy, perform routine data quality checks, initiate backups, and execute data recovery procedures. |
| IT Department | Maintain EHR system security, manage storage, schedule backups, and oversee disaster recovery processes. |
| Compliance Officer | Monitor adherence to regulatory requirements and organizational policies regarding EHR data handling. |

## 4. Procedures

### 4.1 EHR Data Entry

1. Log in using assigned credentials and two-factor authentication.
2. Verify patient identity (full name, DOB, unique identifier) before data entry.
3. Enter patient information accurately and completely at the point of care or as soon as possible after the encounter.
4. Use standardized formats and approved medical terminologies (e.g., SNOMED, ICD-10).
5. Review the entered data to ensure correctness and completeness.
6. Submit the record; log out of the EHR system after use.

### 4.2 Data Verification & Validation

- Conduct daily audits of randomly selected records to detect errors or inconsistencies.
- Flag and correct inaccuracies promptly, documenting amendments as per policy.
- Maintain a log of data corrections for compliance and quality assurance purposes.

### 4.3 Routine Data Backups

1. Schedule automatic full backups at least daily; incremental backups every 4 hours.
2. Store backup copies at a secure, off-site location and in encrypted cloud storage.
3. Verify backup integrity weekly and document status in the backup log.

### 4.4 Secure Storage of EHR Data

- Ensure EHR servers are protected by firewall, antivirus, and access control measures.
- Restrict access to authorized personnel via role-based permissions.
- Encrypt data at rest and in transit.
- Monitor the system for unauthorized access or potential breaches.

### 4.5 Data Recovery Procedures

1. In event of data loss or system failure, notify IT Department immediately.
2. Initiate data recovery from the most recent valid backup, following the disaster recovery plan.
3. Document the incident, recovery steps taken, systems affected, and corrective action implemented.
4. Report significant incidents to Compliance Officer and senior management.

## 5. Compliance & Review

- All staff must complete annual training on EHR procedures and data security.
- This SOP will be reviewed annually or upon significant changes to technology or regulations.

## 6. References

- HIPAA Privacy and Security Rules
- Organization's Data Protection Policy
- Relevant state and federal healthcare regulations

## 7. Revision History

| Version | Date | Description | Author |
|---|---|---|---|
| 1.0 | 2024-06-15 | Initial SOP Release | Quality & Compliance Team |