Standard Operating Procedure (SOP)

Secure Handling and Storage of Medical Records

This SOP details the **secure handling and storage of medical records**, covering procedures for accessing, managing, and storing patient information to ensure confidentiality, integrity, and compliance with legal and regulatory standards. It includes guidelines for physical and electronic record security, authorized access controls, record retention and disposal practices, and protocols for breach prevention and incident reporting. The objective is to protect sensitive medical data from unauthorized access, loss, or damage while maintaining accurate and accessible records for healthcare delivery and auditing purposes.

1. Purpose

To establish standardized practices for securely handling, storing, and disposing of medical records, ensuring patient privacy, data integrity, and regulatory compliance.

2. Scope

This SOP applies to all employees, contractors, and authorized personnel who access, manage, or store physical or electronic medical records within the organization.

3. Definitions

- **Medical Records:** Any documents containing personal health information (PHI), either in paper or electronic format.
- **Authorized Personnel:** Individuals granted access rights to patient information based on job responsibilities.
- **PHI:** Protected Health Information, as defined under HIPAA and relevant regulations.

4. Responsibilities

- **Records Custodian:** Oversee implementation of this SOP and ensure ongoing compliance.
- **All Staff:** Adhere strictly to access, handling, and storage protocols.
- **IT Department:** Maintain IT security controls, conduct regular audits, and support electronic record access.

5. Procedures

- **5.1 Physical Record Security**
  - Store records in locked cabinets/rooms with restricted access.
  - Keep storage areas monitored using surveillance and alarm systems.
  - Do not leave records unattended in public or unauthorized areas.
- **5.2 Electronic Record Security**
  - Use encrypted systems and secure authentication (e.g., passwords, biometrics).
  - Restrict user access based on roles and responsibilities (principle of least privilege).
  - Implement regular data backups and disaster recovery processes.
- **5.3 Access Control**
  - Grant access to records only to authorized personnel.
  - Maintain a log of all access and modifications to medical records.
  - Conduct regular reviews and audits of access privileges.
- **5.4 Record Retention and Disposal**
  - Follow regulatory guidelines for record retention periods.
  - Securely dispose of records using shredding (paper) or digital erasure (electronic data).
  - Document all disposal activities for audit purposes.
- **5.5 Breach Prevention and Incident Reporting**
  - Train staff in data protection principles and breach detection.
  - Immediately report any suspected or actual breaches to the compliance officer.
  - Conduct incident investigations and notify regulatory authorities as required.

6. Compliance & Monitoring

- Conduct regular training and awareness programs for all personnel.
- Perform routine audits of medical record storage, access, and disposal practices.
- Document compliance with HIPAA, GDPR, and other relevant laws.

7. Review & Revision

This SOP will be reviewed annually, or as needed, to ensure ongoing effectiveness and compliance with evolving regulations and best practices.

8. References

- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- Organization Policies and Procedures