SOP: Auditing and Monitoring of Patient Data Access

1. Purpose

This SOP defines the procedures for **auditing and monitoring of patient data access**, including the systematic tracking of access to electronic health records, ensuring compliance with privacy regulations, identifying unauthorized or suspicious activities, maintaining detailed access logs, conducting regular reviews and audits of access records, and implementing corrective actions to safeguard patient confidentiality and data integrity. The purpose is to protect sensitive patient information by enforcing strict access controls and continuous monitoring.

2. Scope

This SOP applies to all staff and third-party vendors who have authorized access to patient electronic health records (EHRs) and related health information systems within the organization.

3. Responsibilities

- **Privacy Officer:** Oversees the implementation and enforcement of data access policies.
- **IT Department:** Maintains access monitoring tools, access logs, and supports audit activities.
- **Managers:** Ensure staff awareness of data access policies and their responsibilities.
- **All Users:** Comply with established access procedures and report any unauthorized access.

4. Definitions

Term	Definition
Electronic Health Records (EHR)	Digital version of a patient's paper chart, maintained by health professionals.
Access Log	Detailed record of user access and activity within EHR systems.
Audit Trail	A chronological set of records that provide documentary evidence of user activities.

5. Procedures

1. **Access Logging:**
    - Enable automated logging of all user access to patient records within EHR systems.
    - Record details such as user ID, time and date, patient data accessed, and activity performed.
2. **Regular Monitoring:**
    - IT or designated privacy staff review access logs daily for anomalies or unauthorized access.
    - Use automated tools to flag suspicious activities, such as unusual hours or volume of access.
3. **Audit Reviews:**
    - Conduct formal audits of access logs at least quarterly, and spot-check records as needed.
    - Document findings and maintain audit records for a minimum of 6 years.
4. **Incident Response:**
    - Investigate any unauthorized or suspicious access within 24 hours and document findings.
    - Report breaches according to organizational and legal requirements.
5. **Corrective Actions:**
    - Implement necessary corrective or disciplinary actions in response to audit findings.

- Review and update access controls and policies accordingly.

6. Documentation and Recordkeeping

- All access logs, audit trails, and investigation records must be maintained in secure, tamper-evident storage.
- Records are retained according to applicable legal and policy requirements (minimum 6 years recommended).

7. Training and Awareness

- All relevant staff must receive initial and periodic refresher training on data access, monitoring, and privacy obligations.
- Training records are to be maintained by HR or the Privacy Officer.

8. Review and Revision

- This SOP will be reviewed annually or upon significant change in regulations or organizational processes.
- Document revisions, including dates and responsible parties.

9. References

- HIPAA Security and Privacy Rules
- Organization's Data Access and Security Policies
- Applicable State and Federal Laws

10. Approval

Name	Title	Date	Signature