SOP Template: Reporting and Incident Management for Breaches of Health Records

This SOP details the **reporting and incident management for breaches of health records**, including identification and classification of breaches, immediate response actions, notification procedures to relevant authorities and affected individuals, investigation and root cause analysis, documentation and record-keeping, corrective and preventive measures, staff training and awareness, and continuous monitoring to safeguard the confidentiality and integrity of health data.

1. Purpose

To set forth standardized procedures for reporting, managing, and mitigating breaches of health records, ensuring timely response, compliance with legal and regulatory requirements, and ongoing improvements to data protection processes.

2. Scope

This SOP applies to all personnel, departments, and third-party vendors who have access to health records within the organization.

3. Definitions

- **Health Record Breach:** Unauthorized access, disclosure, alteration, or destruction of health records.
- **Incident:** Any actual or suspected compromised confidentiality, integrity, or availability of health records.

4. Responsibilities

- All staff are responsible for immediately reporting suspected or known breaches to the Data Protection Officer (DPO) or designated authority.
- The DPO is responsible for coordinating the response, notification, documentation, and corrective actions.

5. Procedure

1. **Identification and Classification**
    - Staff must promptly report any actual or suspected breach to their supervisor and the DPO.
    - Incidents are classified based on severity, impact, and sensitivity of the data involved.
2. **Immediate Response Actions**
    - Contain the breach by suspending compromised accounts, limiting access, or isolating affected systems.
    - Preserve evidence for subsequent investigation.
3. **Notification Procedures**
    - Notify top management, IT, compliance, and relevant authorities as per applicable laws.
    - Inform affected individuals without undue delay, outlining the nature of the breach and recommended actions.
4. **Investigation and Root Cause Analysis**
    - Conduct a thorough investigation to ascertain the breach's origin, impact, and exploit methods.
    - Document findings and risks to health record confidentiality, integrity, and availability.
5. **Documentation and Record-Keeping**
    - Maintain a breach register capturing incident details, actions taken, and notification records.
    - Securely store all related evidence and correspondence.
6. **Corrective and Preventive Measures**
    - Implement measures to prevent recurrence based on investigation outcomes.
    - Update policies, technical safeguards, and access controls as needed.
7. **Staff Training and Awareness**
    - Conduct training sessions on data protection, breach recognition, and incident reporting procedures.
    - Regularly distribute awareness materials and reminders on health record confidentiality.
8. **Continuous Monitoring and Review**
    - Monitor systems for unauthorized access or anomalies.
    - Review and update this SOP annually or after major incidents.

6. Documentation Template

Field	Description
Incident ID	Unique identifier for the breach
Date & Time Detected	When the breach was identified
Reporter	Name and role of person reporting
Description	Details of the breach incident
Classification	Severity and impact assessment
Immediate Actions Taken	Steps to contain the breach
Authorities Notified	Names and contact details
Individuals Notified	Details of patient/individual notification
Investigation Findings	Summary of root cause & outcomes
Corrective Actions	Preventive steps implemented

7. Review and Updates

This SOP should be reviewed at least annually or following any major incident to ensure effectiveness and compliance with evolving regulations and standards.