Fidesic

www.fidesic.com

FIDESIC SECURITY INCIDENT PROCEDURES POLICY

Table Of Contents

Document ID: **PR.IP-9**
Effective Date: 5-23-2024
Reviewed Date:4-15-2025
Version: 1.0

Purpose

The purpose of this policy is to establish procedures for addressing security incidents to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This policy aims to promptly identify, respond to, mitigate, and document security incidents.

Scope

This policy applies to all employees, contractors, and third-party agents who handle protected health information (PHI) within Enliven Software

Definitions

- **Security Incident**: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- **PHI**: Protected Health Information as defined by HIPAA.

Responsibilities

- **Security Officer**: Responsible for the overall management and execution of this policy, including incident response coordination.
- **IT Department**: Responsible for technical aspects of incident detection, response, and mitigation.
- **All Staff**: Responsible for reporting suspected security incidents.

Procedures

Incident Identification

Monitoring: Implement monitoring mechanisms to detect potential security incidents.
Reporting: Employees must report suspected incidents to the Security Officer immediately.

Incident Response

- **Initial Assessment**: The Security Officer will conduct an initial assessment to confirm if a security incident has occurred.

- **Containment**: Actions will be taken to contain the incident and prevent further damage.
- **Investigation**: A thorough investigation will be conducted to determine the scope, cause, and impact of the incident.
- **Mitigation**: Appropriate steps will be taken to mitigate the effects of the incident.

Documentation

- **Incident Report**: An incident report will be created for each security incident, detailing the nature, scope, and resolution of the incident.
- **Logging**: All actions taken during the incident response will be logged for future reference and compliance purposes.

Notification

- **Internal Notification**: Key stakeholders within the organization will be notified of the incident.
- **External Notification**: If required, affected individuals and regulatory bodies will be notified in accordance with HIPAA regulations.

Post-Incident Review

- **Analysis**: Conduct a post-incident review to analyze the incident and identify any weaknesses in security controls.
- **Improvement**: Implement corrective actions and improvements to prevent future incidents.

Training

All employees will receive regular training on security incident procedures and their role in reporting and responding to incidents.

Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

Review and Revision

This policy will be reviewed regularly and revised as necessary to ensure continued compliance with HIPAA regulations and alignment with industry best practices.