SECURE HIT SECURE HEALTH INFORMATION TECHNOLOGY		**Security Incident Response and Report Policy and Procedure**
Category: Administrative Safeguard		P & P #: 2024
Prepared By: e-Signature on file Jose Miranda ISSO	**Revised By: e-Signature on file** José Miranda ISSO	**Approved By: e-Signature on file** Janet Rios, CEO
Effective Date: May 2018 Last revision: Jan 2024	Expiration Date: N/A	Page 1 of 3

1. Definitions

Electronic Health Information (EHI): Electronic protected health information and any other information that identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual and is transmitted by or maintained in "electronic media," as defined in 45 CFR § 160.103, that relates to an individual's past, present, or future health or condition; the provision of medical care to an individual; or past, present, or future payment for the provision of health care to an individual. Electronic Protected Health Information (ePHI): Has the meaning assigned in 45 CFR § 160.103.

ePHI - "Electronic Protected Health Information" - Health information in electronic format, relating to an individual or patient, as defined in the federal HIPAA Security Rule.

P&P - Policy and Procedure

IaaS - Infrastructure as a Service

ISO – Information System Officer

ISSO – Information System Security Officer

BYOD - Bring Your Own Device

IT - Information Technology (Information Systems).

Minimum Necessary Requirements – means the provision in the HIPAA Rules that, under certain circumstances, requires a Covered Entity or Business Associate to use reasonable efforts when Using or Disclosing PHI or requesting PHI from another Covered Entity or Business Associate to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or request. See 45 CFR §164.502 (b) and §164.514 (d).

Authorization Procedure – is a recommended implementation specification and is defined within the Occupational Security Standard (164.308(a)(3)) and falls under the category of Administrative Safeguards defined in the HIPAA Security Rule.

2. Purpose

This Security Incident Response Plan exists to ensure that the Secure Health Information Technology Corp. (SecureHIT) is prepared to handle cyber incidents effectively and efficiently. Security incidents are more frequent and sophisticated than ever. No organization worldwide is immune to attacks. Organizations must ensure that they are prepared to respond to incidents, as well as to prevent and detect them. By having a plan, a team, and conducting exercises, organizations will be better prepared for unavoidable incidents and will be able to contain the damage and mitigate additional risk to the organization. Resources must be deployed in an organized manner with skills exercised and communication strategies.

This document describes the general plan for responding to security incidents at SecureHIT. It identifies the structure, roles and responsibilities, types of common incidents, and the approach to prepare, identify, contain, eradicate, recover, and carry out lessons learned in order to minimize the impact of security incidents.

The goal of the Security Incident Response Plan is to ensure that organizations are organized to respond to security incidents effectively and efficiently.

3. Scope

This security incident response plan applies to all networks, systems, and data, as well as organization members, employees, and contractors, as well as vendors who access the networks, systems, and data. Members of the organization who may be called upon to lead or participate as part of the Security Incident Response Team should be familiar with this plan and be prepared to collaborate with the goal of minimizing adverse impact on the organization.

4. Policy

The ISO will create and maintain procedures to identify and monitor security incidents. These can be classified as serious or non-serious;

4.1. A non-serious incident has the following characteristics:
- 4.1.1. Did not have malicious intent or the attack was not directed directly at SecureHIT and,
- 4.1.2. It was determined that the sensitive information in the SecureHIT, specifically ePHI, was not used, disclosed, or damaged.

4.2. A serious incident has the following characteristics:
- 4.2.1. Had malicious intent or the attack was directed directly at SecureHIT and,
- 4.2.2. It was determined that SecureHIT sensitive, confidential, or protected information, specifically ePHI, may have been used, disclosed, or damaged.

All members of the workforce, contractors, volunteers and/or students must report any potential security incident to ISO or ISSO within 2 hours of alarm generation or notification. A potential security incident is an occurrence that poses a deviation from established policies and procedures or any activity that could potentially jeopardize sensitive information, specifically ePHI, to unauthorized use, disclosure, or modification.

5. Procedure

Refer to the Security Incident Response Plan 2024.

6. Responsibilities

Responsibility for the security of protected health information rests with the Executive Director of SecureHIT, Janet Ríos. During times when a high or critical security incident occurs, this responsibility is entrusted to the SecureHIT ISSO.

All members of the workforce will be responsible for:

- Prevent potential security incidents
- Identify any potential safety incident
- Report any security incident to the Information System Security Officer
- Assist the Information System Security Officer in dealing with the incident and
- mitigate its damaging damages, if possible

The Information System Officer, under the delegated authority of the Chief Executive Officer, will be responsible for:

- Maintain and update all policies and procedures related to security incidents

- Classify all incidents as serious or not serious as established in this policy
- Maintain and update procedures to respond to security incidents
- Document all reported incidents and their resolution

The Information Systems Security Officer, under the supervision of the Director of Information Systems, will be responsible for:

- Implement and maintain the controls and safeguards established in this policy.
- Maintain the necessary procedures to support this policy.
- Ensure and support compliance by the workforce.

All members of the workforce, contractors, volunteers, and/or students will be responsible for complying with the requirements of this policy.

7. Compliance

Failure to comply with this or any other security procedure may result in disciplinary action under the Sanction Policy. SecureHIT may make referrals to relevant state and federal agencies with jurisdiction over the laws and regulations associated with the violations.

The Security Incident Procedure supports SecureHIT compliance with the corresponding standard in the Administrative Safeguards category of the HIPAA Security Rule.

REVISIONS

Contact:	Title:	Date:	Comments:
Janet Rios Colon	Chief Executive Officer	May 2018	
Janet Rios Colon	Chief Executive Officer	Nov 2018	
Janet Rios Colon	Chief Executive Officer	April 2020	
Jose Miranda	ISSO	June 2021	
Jose A. Miranda	ISSO	June 2022	
Jose A. Miranda	ISSO	Jan 2023	

SECURE HIT SECURE HEALTH INFORMATION TECHNOLOGY		**Security Incident Response and Report Policy and Procedure**
Category: Administrative Safeguard		P & P #: 2024
Prepared By: e-Signature on file Jose Miranda ISSO	**Revised By: e-Signature on file** José Miranda ISSO	**Approved By: e-Signature on file** Janet Rios, CEO
Effective Date: May 2018 Last revision: Jan 2024	Expiration Date: N/A	Page 1 of 3

Jose A. Miranda ISSO Jan 2024

REGULATORY REFERENCE

HIPAA Final Security Rule, 45 CFR 164.308 (b) (1), 45 CFR 164.308 (b) (2) and 45 CFR 164.308 (b) (3), Department of Health and Human Services.

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:10:02 -04'00'