SECURE HIT SECURE HEALTH INFORMATION TECHNOLOGY		**DISASTER RECOVERY POLICY**
Category: Administrative Safeguard		P & P #: 2024
Prepared By: e-Signature on file Samuel rivera, ISO	**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

1.0 PURPOSE

This plan is aimed at detailing dangerous situations that may interrupt the normal service and/or office operations such as:

- Fires
- Floods
- Earthquakes
- Pandemic or biological threatening
- Bomb threat or bomb explosion
- Civil disobedience
- Riots and demonstrations inside or outside the building
- Environmental conditions
- Natural disasters that may affect employees when they arrive, stay or leave work.
- Earthquake
- Pandemic
- National emergency

Detailing the response to these situations, but not limited to these.

The purpose is to establish and implement policies and procedures to respond in the event of an emergency (eg. fire, vandalism, system failures or natural disaster) that cause harm to systems that process, store or transmit ePHI from Secure Health Information Technology Corp. (SecureHIT) and any other information system.
The contingency plan is used to respond to an emergency in the information systems and includes making safeguards of information, preparing critical facilities and detailing migration plans that can be used to facilitate the continuity of operations in the event of an emergency or disaster.

The purpose is to establish and implement, as necessary, procedures to restore any lost data.

2.0 SCOPE

This policy applies to the entire SecureHIT workforce and to all computer systems and services that process, store or transmit ePHI.

3.0 POLICY

Recovery Plan Policy
The Information Systems Officer shall establish information retrieval procedures, including related methods, tools and controls, which are consistent with the following elements:

- A risk analysis related to continuity of operations
- The recovery times of the company's processes
- The recovery strategy of the company

The information retrieval procedures will specify the steps to follow in the following areas:

- Activation of the disaster recovery plan
- Notification to the personnel responsible for the information recovery processes
- Physical access to the backups generated according to the Data Backup Policy and Procedure
- Recovery of the backups using the methods, tools and technologies available in the different scenarios in which the disaster recovery plan could be activated

SecureHIT will evaluate and update the information retrieval procedures each time an assessment of the business contingency plan is made or when changes are made to the methods, frequency and controls related to the generation, storage and retrieval of the backups.

4.0 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 the information can be used to identify the individual and is transmitted by or maintained in “electronic media,” as defined at 45 CFR § 160.103, that relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Electronic Protected Health Information (ePHI): has the meaning assigned to such term at 45 CFR § 160.103.

ePHI - “*Electronic Protected Health Information*” – Health Information in electronic form, related to an individual or patient, as defined in the Safety Rule of the federal HIPAA law.

P&P - Policy and Procedure

5.0 PROCEDURE

Refer to the Disaster Recovery Plan 2024.

6.0 RESPONSIBILITIES

The Information Systems Officer, under the authority delegated by the Chief Executive Officer, will ensure the implementation of all elements of this policy and related procedures

7.0 COMPLIANCE

Failure to comply with this or any other security policy 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 Disaster Recovery Policy supports SecureHIT compliance with the corresponding required implementation specification in the Administrative Safeguards category of the HIPAA Security Rule.

8.0 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	Aug 2020	
Jose A. Miranda	ISSO	June 2021	
Jose A. Miranda	ISSO	June 2022	
Jose A. Miranda	ISSO	Jan 2023	
Jose A. Miranda	ISSO	Jan 2024	

9.0 REGULATORY REFERENCES

HIPAA Final Security Rule, 45 CFR 164.308(a)(7)(i), Department of Health and Human Services.

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:06:44 -04'00'