SECURE HIT SECURE HEALTH INFORMATION TECHNOLOGY		**DISASTER RECOVERY PLAN**
Category: Administrative Safeguard		P & P #: 2024
Prepared By: e-Signature on file Janet Rios CEO	**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 7

1.0 PURPOSE

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.

This contingency plan and procedure should be invoked for all identified impacts, including emergency mode operation.

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 SUMMARY

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

2.1 Fires
2.2 Floods
2.3 Bomb threat or bomb explosion
2.4 Civil disobedience
2.5 Environmental conditions
2.6 Natural disasters that may affect employees when they arrive, stay or leave work
2.7 Human Error
2.8 Equipment failure
2.9 Thief
2.10 Act of terrorism
2.11 Earthquake

2.12 Pandemic
2.13 National emergency

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

3.0 SCOPE

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

4.0 COMMITTEE

4.1. Assigned Personnel for Emergency and Recovery Committee
- 4.1.1. Janet Ríos Colón - President and Chief Executive Officer C. (787) 562-7036
- 4.1.2. Samuel Rivera - Information System Administrator C. (787) 234-4330
- 4.1.3. José Miranda - Information System Security Officer C. (787) 553-3354
- 4.1.4. Maria J Díaz - Customer Service Officer C. (787) 392-5799

5.0 PLAN

5.1. Contingency plan in case of disaster.

- 5.1.1. In case of imminent warning emergencies due to inclement weather, for example, natural disaster, fire, flood, earthquake, hurricane, tsunami, sabotage, etc.), where the local area could be affected and ensuring the wellbeing of SecureHIT workforce and staff, the following measures will be taken:
- 5.1.2. In the case of anticipated events, once the warning of the event has been issued, this disaster contingency plan is activated.
  - 5.1.2.1. Remote service release is sent.
  - 5.1.2.2. All SecureHIT services reside in the Amazon Web Service and Google Suite cloud. Therefore, the communication indicates the internet connection that the employee must access and could work from the safest place as identified by the employee, before and after the emergency.
  - 5.1.2.3. In said statement, the method will be indicated to keep in touch with the President/CEO on a daily basis.
  - 5.1.2.4. SecureHIT calls are transferred to the corporate cell.

5.1.2.5. The Emergency and Recovery Committee will contact the System Administrator and/or the persons designated by the Executive Officers, to re-evaluate the status of the online services and the ability to re-establish operations. This depends on Puerto Rico communications situations, for local clients. To the extent that SecureHIT resides on AWS our services are not limited to the availability of local communication.

5.2. Restore the operation:

5.2.1. The Emergency and Recovery Committee will inspect the conditions in which it is located to operate.

5.2.2. In the case of a total interruption of communications on the island for a long time (read more than a week);

5.2.3. The Emergency and Recovery Committee will determine the corresponding alternate place to continue operations and the SecureHIT communications system will be temporarily enabled until the communications are reestablished.

5.2.4. In case the communication breakdown is extensive, and the only alternative is the temporary alternate we proceed to restore the data that is stored in the vault for local Puerto Rico clients.

5.2.5. The Network Administrator in coordination with the CEO will proceed to verify the critical equipment necessary for the operation according to the following checklist:

5.2.5.1. Servers

5.2.5.2. SecureHIT Hardware and Software Inventory

5.2.5.3. Communications Status:

5.2.5.3.1. Puerto Rico (island wide) Communications Status

5.2.5.3.2. Staff Internet Connections

5.2.5.3.3. Cell Phone communications

5.2.5.4. Alternate Site

5.2.5.4.1. Status of Service for server restore

5.2.6. The Developers Consultants in coordination with the CEO will proceed to verify the functionality of the equipment (rented service) and the critical applications necessary for the operation in the data center according to the following checklist:

5.2.6.1. Servers operating service (AWS linux, Ubuntu)

5.2.6.2. AWS virtualization tool
5.2.6.3. Servers AMI
5.2.6.4. Database snapshot
5.2.6.5. Communications (Internet, Email and Telephone)
5.2.6.6. Restore the AMI
5.2.6.7. Restore Snapshot
5.2.6.7.1. Database
5.2.6.7.1.1. SecureHIT production,
5.2.6.7.1.1.1. Direct SecureHIT
5.2.6.7.1.1.2. API
5.2.6.8. Route 53 AWS service manage the DNS services

5.2.7. The authorized persons to access the AWS Console, the CEO will designate who will access copies of the identified programs, database and access codes.

5.2.8. Once the communication with Amazon Web Service has been restored, the following steps will be taken:

5.2.8.1. For Amazon Web Service, under the SecureHIT account, the restoration using AWS load balancer restoration will occur automatically.
5.2.8.2. Contact
5.2.8.2.1. Samuel Rivera srivera@securehitpr.com (787)234-4330
5.2.8.2.2. José Miranda jmiranda@securehitpr.com (787)553-3354
5.2.8.3. Route 53 AWS service manages the DNS services.

Note: ALL THE NECESSARY INFORMATION OF CONFIGURATION AND ACCESS RESIDES IN THE SUPPORT FOLDER IN GOOGLE DRIVE.

- In the absence of communication services, the CEO and/or delegate will proceed to contact the Internet and Telephone Service Provider to ensure they are restored. SecureHIT will require our suppliers for internet access, office space in the company's facilities, if SecureHIT does not have access to the Internet.
- Once the communications are enabled, the Network Administrator will verify the availability of the portals and communication services by performing the connection tests. This will proceed to inform the Executive Officer of SecureHIT and the department supervisors the availability of the SecureHIT systems for the operations of the users.

- The clients will proceed to restart the operations of their service according to their communications access.
- The Emergency and Recovery Committee will meet to evaluate the recovery process of the event, documenting the findings on a Recovery Plan Evaluation Sheet.

6.0 PROCEDURE

6.1. In the event that the production region in North Virginia 'us-east-1' is out of line will proceed to activate the backup region in Northern California 'us-west-1'

6.1.1. On the AWS console change the region and select 'US West (N. California)'. https://signin.aws.amazon.com/

6.1.2. Go to the EC2 console where the AMI's (AWS Machine Image) are located and press Launch.

6.1.3. Enter the parameters corresponding to the Northern California VPC and the type of instance. Repeat step 3 for the number of instances that it is necessary to restore in Northern California.

6.1.4. Once all the instances are online, it must be confirmed that the services are functional as well as the connectivity from the internet to the servers that require it.

6.2. RollBack Procedure; for more details refer to Rollback Procedure.

6.2.1. In the event that an event occurs in which one or more instances have to be restored, the backup will be restored.

6.2.2. From the AWS console change the region and select 'US East (N. Virginia)'. https://signin.aws.amazon.com/

6.2.2.1. Go to the EC2 console where the AMI's (AWS Machine Image) are located and press Launch.

6.2.2.2. Enter the parameters corresponding to the VPC of Virginia and the type of instance. Repeat step 3 for the number of instances that it is necessary to restore in North Virginia.

6.2.2.3. Once all the instances are online, it must be confirmed that the services are functional as well as the connectivity from the internet to the servers that require it.

7.0 DEFINITIONS

Command center - The Emergency Command Center will be remote and using all the available communications methods. Any potential danger must be reported to the Emergency and Recovery Committee. Personnel assigned to crisis management will meet as many times as necessary to respond or issue appropriate instructions from management. If an emergency situation occurs, outside working hours, it is imperative to communicate such a situation and the status in which the employee is to his immediate supervisor.

Threat to facilities - When a threat is received, the recipient should obtain as much information as possible.

Emergencies due to natural disaster or weather - A radio station that warns about weather conditions is tuned by the company's Emergency and Recovery Committee to keep it informed about the possibility of adverse and severe weather conditions.

CEO - Chief Executive Officer

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 terms 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

8.0 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.

9.0 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 Plan supports SecureHIT compliance with the corresponding required implementation specification in the Administrative Safeguards category of the HIPAA Security Rule.

10.0 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	July 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	

11.0 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 12:06:21 -04'00'