<<organization>>

Contingency Planning Policy

Effective Date:

Purpose

The purpose of this policy is to define [ORGANIZATION] Contingency Planning process and to define the activities that should be performed to minimize the impact of a potentially damaging event on the information technology environment and organization. The purpose of a contingency plan is to allow an organization to return to its daily operations as quickly as possible after an unforeseen event. The contingency plan protects resources, minimizes customer inconvenience and identifies key staff, assigning specific responsibilities in the context of the recovery. For example, human resources may develop employee evacuation plans; support employee benefits programs, such as health care or worker's compensation; or hire temporary workers as needed. This includes the procedures for performing disaster recovery testing and contingency planning review and update. The Disaster Recovery testing and Contingency Plan review procedures are executed so that in the event of a disaster, continuation of critical business processes and the protection of electronic personal health information is maintained.

Policy Statement

A Contingency Plan endeavors to protect the confidentiality, integrity and availability of PHI during an emergency situation such as a power loss, earthquake, etc. Senior leadership has overall responsibility for contingency planning, including funding the work to develop, test and maintain the plan. The Compliance Officer and/or Contingency Plan Coordinator have overall responsibility for developing and maintaining the plan. The Coordinator communicates with staff and trains them on the plan and their responsibilities.

The plan will be tested on a regular basis using mock situations to identify problems and areas for improvement and update the plan to reflect changes in the organization and technology. Any Stake-holders' issues and regulatory requirements are also incorporated into the planning process.

A contingency plan should be developed by:

1. Identifying the functional areas essential to business operations.
2. Determining how each situation, such as fire or flood, would affect these key areas; what actions would be taken; and the resources needed for each one.
3. Setting goals for the return to essential operations and return to full normal operations.
4. Identifying each required process and document each step in the process, what needs to be done, along with the staff and other resources needed to complete the work. Develop plans for each functional area and the organization as a whole
5. Implementing a communications and education plan to keep employees informed of changes and remind them of their roles and responsibilities.

Policy Owner

1. [ROLE]

Standards

The organization should maintain a Contingency Plan that includes:

- Business Impact Assessment
- Contingent Operations Process
- Data Backup Process
- Disaster Recovery Plan
- Emergency Operations Process

1.0 Prepare Contingency Plan for Emergency Situations

- Develop [ORGANIZATION] overall contingency objectives, including services to be provided with critical timeframes.
- Utilizing PHI inventory, identify critical systems and processes
- Perform Business Impact Analysis to determine the criticality of infrastructure, applications and data.
- For each system and process develop an alternative manual or automated process to continue critical business operations and ensure the integrity of organization data, including PHI.
- Establish roles and responsibilities and organization framework for developing, implementing and managing Contingency Plans.

2.0 Complete the Data Backup Plan

- Identify information systems (e.g. applications, databases) that contain PHI.
- Develop Backup Strategy for systems that contain PHI.
- Develop process for creation and maintenance of retrievable copies of PHI including data, images, voice or video files.
- Store all media used in backing up PHI in a physically secure environment different from the location of the computer systems it backed up.
- Develop guidelines and procedures for periodically testing backups to ensure PHI data can be retrieved and made available.

3.0 Complete Disaster Recovery Plan

- Develop procedures and processes necessary to restore systems, databases and applications from data backups in case of an emergency.
- Develop procedures to log system outages, failures and data loss to critical systems.
- Train all staff on their roles and responsibilities in case of an emergency situation.

4.0 Develop and Implement Emergency Mode

- Develop emergency procedures that identify the actions to be followed after an incident which jeopardizes business operations and/or human life.
- Develop fallback procedures to move essential business operations to an alternative location.
- Create resumption procedures which describe the actions to be taken to return to normal business operations.

- Develop and implement a training program to train staff members on Emergency Mode Operations.
- Establish guidelines to periodically test Emergency Operations.

5.0 Develop Contingency Plan Test procedures

- Develop a set of tabletop scenarios that will be used to test the Emergency Mode, Data Backup and Disaster Recovery sections of the plan.
- Set a schedule for annual testing of the contingency plan.
- Create a Contingency Plan Test Report with analysis of the results of the tests.

References

Internal

1. PHI Protection Policy

External

1. 45 C.F.R. § 164.310 (a)(7)(i): Contingency Plan. Standard: Establish and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
2. 164.308(a)(7)(ii)(A) Data Backup Standard: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
3. 164.308(a)(7)(ii) (B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
4. 164.308(a)(7)(ii) (C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
5. 164.308(a)(7)(ii) (D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.
6. 164.308(a)(7)(ii) (E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.
7. 164.310 (A)(2)(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.