Contingency Plan

**Purpose:**

Per the HIPAA Security Rule [§ 164.308(a)(7)], this policy has been established to produce rules for continuing business without the normal resources of the organization.

**Definitions:**

1. Data Classification:
   1. Mission Critical: Any lack of availability of data has a significant and immediate impact on the treatment of patients. Examples include clinical systems like medical transcription, nursing, lab, radiology, or pharmacy.
   2. Essential: Required for normal day-to-day operations, but do not directly affect patient care. Examples include materials management, billing, or accounts payable.
   3. Important: Required for operations, but will not prevent patient care or long term functioning. Examples include messaging systems or management reporting systems.
   4. Low: Useful but not essential systems. Examples include marketing, volunteer check-in, or websites. Note that each organization must determine its own classification because a payer may find that messaging is a mission critical application where a provider would rate this much lower.
2. Disaster (Information System): An event that makes the continuation of normal information system functions impossible; an event which would render the information system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).
3. Disaster Recovery Coordinator (DRC): Individual assigned the authority and responsibility for the implementation and coordination of IS disaster recovery operations.
4. Disaster Recovery Plan: The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
5. Recovery Point Objective (RPO): The point in time to which systems and data must be recovered after an outage, as determined by the responsible business unit(s). RPO is measured in hours or days, as an answer to the question, ‘How many (hours or days) old can the recovered data be?’ or “How recent (hours or days) must the recovered data be?’ or ‘How much data are you willing to lose?’ RPO is the point in time to which data must be restored in order to resume processing.
6. Recovery Time (RT): The number of hours or days in which you want to recover a resource or resume a business activity. For example, you might determine that customer service must be functioning again after an interruption within one (1) day. The RT is one (1) day. You might decide, on the other hand, that the RT for your email system is four (4) hours. In some Internet businesses, an RT might be measured in minutes. RT is the amount of down time before outage threatens survival of the organization/mission critical processes.
7. Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices; an adverse event whereby some aspect of computer security could be threatened; an IS Disaster would be considered a security incident.

**Policy**:

**Data Backup Plan**

1. All ePHI shall be stored on network servers in order for it to be automatically backed up by the system.
2. ePHI will not be saved on the local drives of personal computers.
3. ePHI stored on portable media shall be saved to the network to ensure backup of ePHI data.
4. [Insert Covered Entity or Business Associate Name] will conduct daily backups of user-level and system-level information and store the backup information in a secure location. A weekly backup shall be stored offsite.
5. Each department shall establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all ePHI.
6. The Data Backup Plan will apply to any and all files that may contain ePHI.
7. The Data Backup Plan shall require that all media used for backing up ePHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.
8. If a Business Associate or backup service is used, a written contract is required to ensure that the contractor will safeguard the ePHI in an appropriate manner.
9. Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that exact copies of ePHI can be retrieved and made available.
10. Each department shall submit its new and revised Data Backup Plan to the HIPAA Security Officer for approval.
    1. Backup procedures shall include the following elements:
       1. Definition of which file systems to back up.
       2. Definition of frequency of media rotation.
       3. Definition of off-site storage requirements and frequency.
       4. Documentation and labeling of storage media.
       5. Performing backups before the movement of systems.

**Disaster Recovery Plan**

1. [Insert employee designated to run the disaster recovery plan] will be the Disaster Recovery Coordinator.
2. To ensure that each department can recover from the loss of data due to an emergency or disaster affecting systems containing ePHI, each department will establish and implement a Disaster Recovery Plan pursuant to which it can restore or recover any loss of ePHI and the systems needed to make that ePHI available in a timely manner. Examples include:
   1. Records may be pulled from backup.
   2. If backup records were stored in paper format, paper records may be scanned into the electronic system.
3. The Disaster Recovery Plan includes procedures to restore ePHI from data backups in the case of a disaster causing data loss. May include the different classification levels of data:
   1. Mission Critical information will be pulled first, then, essential, important and low.
4. The Disaster Recovery Plan includes procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.
5. The Disaster Recovery Plan will outline the Recovery Point Objective, or determine how much data can be lost if unavoidable.
6. The Disaster Recovery Plan will outline the Recovery Time. How many minutes, hours days are allowed before everything must be running properly? May include the different classification levels of data:
   1. Mission Critical information will be pulled first, then, essential, important and low.
7. The Disaster Recovery Plan must be made available to the necessary personnel at all times.
8. The disaster recovery procedures outlined in the Disaster Recovery Plan shall be tested on a periodic basis to ensure that ePHI and the systems needed to make ePHI available can be restored or recovered. Examples include:
   1. Data Recovery plan will be tested annually.
9. Each department shall submit its new and revised Disaster Recovery Plan to the HIPAA Security Officer for approval.

**Emergency Mode Operation Plan**

1. Each department shall establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode. Emergency mode operation involves those critical business processes that shall occur to protect the security of ePHI during and immediately after a crisis situation. Examples include:
   1. Critical personnel have been issued emergency response cards for access to the facilities in the event of emergency or disaster.
   2. In the event of power outage, a backup generator will be utilized.
      1. In the event the backup generator doesn’t work, remote access will be utilized by the designated personnel. Information will be printed or transmitted via phone (cell, sat) for patient care.
   3. If facility is under a pre-evacuation, print only necessary documents to maintain proper care for patients.
2. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode. Examples Include:
   1. Emergency Procedures will be tested annually.
3. Each department shall submit its new and revised Emergency Mode Operation Plan to the HIPAA Security Officer for approval.

**11.4 Policy Responsibilities**:

The HIPAA Security Officer shall oversee the creation, evaluation, testing, and updating of the various contingency plans described herein. Each covered component shall submit its new and/or revised procedures and plans to the HIPAA Security Officer for approval and ongoing evaluation. Any procedures developed by covered components shall be consistent with the [Insert Covered Entity or Business Associate Name] HIPAA policies and not deviate from the [Insert Covered Entity or Business Associate Name] standards.