CONTINGENCY PLAN

This Contingency Plan identifies the process to continue operations during emergency or disaster events:

* Emergency Action Plan – Addresses temporary interruption of normal operations such as a power failure at the site or the unavailability of a system containing PHI.

* Disaster Recovery Plan – This plan provides guidance for recovery when a complete disaster situation such as the building or office is destroyed by a fire.

The Plan will be activated when an event occurs which impacts access to PHI needed to provide services for patients or respond to a request from a Covered Entity (CE).

The following position has the authority to activate and part of the Contingency Plan.

- ☐ Business Manager/Administrator
- ☐ Privacy/Security Officer
- ☐ Other: _____

Provided in these plans is the information and guidance needed to respond quickly and efficiently should an unexpected event occur that results in a service interruption for a short or a long period of time. This Plan covers the technical recovery (restoring systems and software), the physical facility repair or replacement and the temporary operating circumstances while working toward normal operations.

To ensure preparedness for emergency response each designated staff member and management team member should have a copy of this plan, including contact lists both in the office and in their homes.

As you plan for your business consider the following

1. Would patient lives be in immediate danger if the business was unable to provide services to CEs? If the answer is yes, having a specific and immediate plan to deal with patient lives is the first priority (patient care plan). Define a patient care plan for the short term.
2. Can you operate from paper for 1-3 days if there is a temporary outage or system loss? If you are unable to operate from paper, how will you deal with responding to clients who provide patient care?
3. Is your system and equipment still available in the marketplace if you need to replace it quickly? If the answer is no, talk to your vendors about your recovery options and the action you need to take now to ensure you would be able to successfully recover all data in the event of a disaster or simple loss of system data. The back-up file you prepare every day cannot be loaded without the correct equipment and software.
4. For a complex technical environment, you may need a more detailed recovery plan.

EMERGENCY OPERATIONS PLAN

An emergency is an event that causes a **temporary** interruption of operations at one or more of your locations. Provide periodic updates to other staff until full service is restored.

In the event of a temporary outage this business will

- ☐ Operate using a paper system until all systems are restored.
- ☐ Operational functions will continue on a manual basis until full service is restored.
- ☐ The following operational functions will be delayed until full service is restored.

  _____

- ☐ Requests for documents or other items stored electronically will be manually recorded for follow-up once the system is restored.
- ☐ Other temporary plans: _____

Procedures for maintaining records while operating under temporary conditions

Recording demographic changes for later entry: _____

Recording requests for appointments for call backs: _____

Procedures for responding to requests for information: _____

Filing claims on paper and/or maintaining information for entering into the system when possible: _____

Other procedures: _____

DISASTER RECOVERY PLAN

A disaster is a major interruption of operations that is likely to continue for multiple days. A disaster may be a system failure that will require multiple days to restore service and system access. It may also be a total destruction of the building and everything in it such as from a fire or hurricane.

Team members assigned to assist in the recovery effort will meet periodically to assess the situation and recommend course corrections. These members will have the responsibility to keep all others informed depending on their needs and roles – emergency services such as fire and police, management, staff and the media. Management and team members should have a copy of the Contingency Plan and all supporting documents both at their homes and work.

Complete the Following Tasks

- ☐ Prepare a call list of all employees. Include name, address, home phone, and cell phone. Create a separate list for each physical site. A copy of the list will be maintained at the office and shared with impacted workers.

- ☐ Select a Control Site for the Disaster Recovery Team to meet immediately after the disaster in the event the office is not available There may also be a need to have an alternate site in the event of a major disaster.

    - ☐ Location of Control Site: _____

    - ☐ Alternate Control Site: _____

- ☐ The Disaster Response Team will include the following key people:

    - ☐ Privacy/Safety Officer
    - ☐ Administrator/Manager
    - ☐ IT Representative
    - ☐ Other: _____

    * Each person should bring a cell phone and personal computer in the event equipment is not readily available for communication purposes.

- ☐ Disaster Recovery Team Member Assignments

    Hardware Vendor Communication _____

    Software Vendor Communication _____

    Patient Care Issues _____

    Utility, Phone, & Media Contact _____

    Other: _____

    _____

- ☐ Complete the equipment/software inventory using the *Hardware, Software & Media Inventory* form located in this Manual – *Forms* section.

- ☐ Prepare a call list of all vendors and equipment suppliers who will be needed in the event of a disaster. Call the individuals on the list to verify that they are the correct contact. The list will be maintained in the facility with this Plan and an additional copy will remain offsite with: _____

  _____

- ☐ Establish a process for emergency access to all PHI and set criteria for reinstitution of normal access controls.

- ☐ Document a data back-up process for all of your systems and files. Obtain directions on the process for a full system restore if indicated by total loss of the facility. Periodically test backed-up data.

Actions If a Disaster Occurs

1. Activate the Call List to notify staff of the disaster and next steps.
2. Convene the Disaster Response team at the Control Site.
3. Documentation – Complete records of the event will be maintained and will include the decisions and activities involved in the recovery process. This documentation will assist with status update and later for audit purposes to improve the recovery process.
4. Assign tasks to individuals and make adjustments as necessary.

   - ☐ Contact the phone company to redirect the phone line to another number or put a message on the line to direct callers to another number or to another facility for care.
   - ☐ Define needs for a permanent facility
     - o If building is destroyed or uninhabitable – Will you repair, replace or lease another facility? Put a team together to deal with a permanent location decision.
     - o Will you continue operations in a temporary site until new permanent facilities are available?
   - ☐ Contact vendors to inform them of the disaster and to arrange for the delivery of the resources and supplies.
   - ☐ Assemble the necessary hardware, software, furniture and supplies to begin the recovery process. Have all back-up media delivered to the Control Site.
   - ☐ Begin the system recovery process:
     - o Assign short-term access if indicated to assist with emergency operations.
     - o Determine the latest back-up files to be restored.
     - o Review and confirm the priority order for installing back-up files and restoring systems.
     - o Inform staff and users of potential recovery times.
     - o Install back-up files and test.

5. Determine the method of acquiring and entering data not on the back-up files. Most back-up processes result in not having the last day of information available and/or you may have to use an older back-up file if the most recent one is damaged or corrupted.
6. Determine the method of adding data gathered during temporary operations.
7. Resume all operational functions. Monitor for appropriate functionality.

Target Schedule for Recovery of Systems and Locations

- Priority systems will be available within _____ hours/days after failure is reported.
- Non-critical systems will be restored within _____ days.

Projected Detailed Timeline for Establishing Temporary Operations

Within 2 hours after notification of a disaster:

- Assess the damage and define the need for an alternate location for a Control Site
- Notify management of the emergency and any other facts or needs already known.
- Follow through on notifications to vendors, staff and others.
- Begin the process to accumulate equipment and software needed if a control site will be set up.
- Review assignments and make changes as necessary.
- Notify "hot site" if applicable. Very large operations may have the need to run an entire duplicate system site (hot site)

Within 4 hours:

- Provide status report to management on the extent of the disaster and the currents plans and schedule for recovery.
- Determine any temporary funding or assistance needed to continue recovery process.
- Confirm that all vendors, employees and other needed resources have been contacted.
- Ensure all utilities have been established or scheduled to allow recovery operations to continue on schedule.

Within 8 hours and continuing for 24 hours

- Status report to management and team members daily.
- Verify that all plans are on schedule with assignments, vendors, etc.
- Review the need to continue or alter plans based on developing information about the process and the disaster.
- Verify that everyone is maintaining an individual log of action to be used in preparing a consolidated log.

Between 24 and 36 hours (depending on recovery schedule established):

- Confirm or adjust the recovery schedule. Make other changes dictated by the schedule.
- Confirm full recovery.
- Initiate a follow up schedule to validate stable operations.
- Determine process for continuous operations in the temporary location. Appointments and claims processing may be handled at the control center or at another site.

Ongoing:

- Continue with status reports until fully operational in permanent location. Frequency of reports can be adjusted.
- Work with team to establish a permanent location.

Test the Disaster Recovery Plan

Name:	Date:	Name:	Date:

1. Call the home of a Recovery Team member after hours and ask them if they have their Employee Call List and Contingency Plan available. Every 6 months is a good time frame for this activity. Record the test date on the master list.
2. Call the numbers on the vendor and supplier contact list to confirm the accuracy of the numbers and that they are still the correct contact for the particular supply. Do this at least annually. Record the test date.
3. Verify the equipment as listed on the Inventory Report at least annually. Record the inventory date.
4. Test the back-up file at least quarterly by working with IT and/or software vendor. Maintain a test log of back-up files. Test all back-up methods to ensure data can be restored.
5. Review the entire Contingency Plan to ensure process is applicable to current operations.
6. Other test plans and their location: _____

CRITICAL DATA BACK-UP PLAN

In order to recover from a major or minor disaster that involves the loss of data, systems should be backed up on a regular basis, preferably daily. Additionally, the back - up media must be available quickly, dictating a storage process with immediate access.

If back-up is provided by a vendor, verify that the vendor has an adequate Contingency Plan and that you understand how to execute a recovery using the back-up files. You will need a Business Associate Agreement with the vendor. Define with the vendor the access, retention, storage and destruction of the back-up media used.

Systems or programs running in the office and back up methods

- ☐ Complete and review the Hardware, Software, and Media Inventory form.
- ☐ List systems in the order of priority you would use to restore functionality following a disaster or system outage. Document name of system and record back up frequency:

System Name/Type of Data	Back up schedule	Storage Location
	☐ Daily ☐ Other	☐ Remote ☐ Other
	☐ Daily ☐ Other	☐ Remote ☐ Other
	☐ Daily ☐ Other	☐ Remote ☐ Other
	☐ Daily ☐ Other	☐ Remote ☐ Other
	☐ Daily ☐ Other	☐ Remote ☐ Other
	☐ Daily ☐ Other	☐ Remote ☐ Other

Staff members responsible for back-up and recovery:

_____

_____

_____

Define back up process:

_____

_____

_____

_____

Testing Schedule:

- ☐ Daily
- ☐ Weekly
- ☐ Quarterly

CALL LIST

This is a call list of all employees and the IT professional(s) who must be notified in the event of emergency/disaster. This list will be reviewed annually and contact information confirmed.

Employee Name	Key Access	Server Access	Home Address	Best Contact Number	Email Address
IT Professional Name	Key Access	Server Access	Home Address	Best Contact Number	Email Address

REVIEW DATES

Name:	Date	Name:	Date:

VENDOR CALL LIST

This is a call list of all vendors and equipment suppliers who will be needed in the event of an emergency/disaster. This list will be reviewed annually, and contact information confirmed.

Name of Company	Contact Name (if applicable)	Phone Number	Equipment	Person Assigned to Call

REVIEW DATES

Name:	Date	Name:	Date: