HIPAA-25: Disaster Recovery Policy

Effective Date:	12-01-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs contingency Disaster Recovery Planning for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations pertaining to disaster recovery, in accordance with the requirements at § 164.308(a)(7).
- HIPAA requires **TCS** to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information.
- A disaster may occur at any time, not necessarily during work hours.
- **TCS** must remain operational with as little disruption of business operations and patient care as possible.
- Continuity of patient care requires uninterrupted access to patient information.
- In a dangerous emergency, evacuating personnel has priority over preserving information assets.
- The following conditions can destroy or disrupt **TCS**'s information systems:
  - Power interruption.
  - Fire.
  - Water.
  - Weather and other natural phenomena, such as earthquakes.
  - Sabotage and vandalism.
  - Terrorism.

Policy Statement

It is the policy of **TCS** to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information in order to be able to reinstall and recover in the case of any data corruption or other disaster within sufficient time to maintain business operations and patient care levels.

Procedures

Preventive Measures:

- The Executive Director and or their designee(s) shall ensure that the following preventive measures, as applicable, are implemented and documented:
  - Back up computer systems and data files according to our Data Backup Policy.
  - Maintain secure backup data in the off-site media vault, according to our Data Backup Policy.
  - Maintain and replace any portable media according to our Data Backup Policy.
  - Test integrity of backup system according to our Data Backup Policy.
  - Disaster Recovery Testing will be conducted on a semi-annual basis to ensure the policy and procedures work effectively as planned. Any lessons learned from this testing will be documented and evaluated for appropriate revisions in the Disaster Recovery policy and procedures.
  - If removable backup media is utilized it should be properly stored and properly labeled.
  - All application systems and data should be prioritized for evacuation as well as disaster recovery process: (red is first priority; yellow is second priority; green is third priority).

- Protect by uninterruptible power supplies all servers, backup systems,and other critical equipment from damage in the event of an electrical outage.
- Locate file servers and other critical hardware in secured rooms with Halon fire protection systems which limit damage to the immediate area of the fire. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
- In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
- In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
- All key staff will be trained in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster on an ongoing basis

❑ The Executive Director or designees must implement and document the following:

- Ensure that major hardware is covered under TCS's property and casualty, and or other appropriate insurance policy or policies.
- Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

Priority Tasks during Emergencies:

<u>As applicable, and under appropriate circumstances, all workforce members should</u>:

- Remain calm.
- Activate the alarm. That is, pull the fire alarm or call 911 as appropriate.
- Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
- If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
- If safe, close all doors as you leave.
- Obtain portable phone(s) to communicate.
- Notify concerned fire, police, security, administration, and others as necessary.
- Notify other departments of situation and emergency protocols.
- If computers have not automatically powered down, initiate procedures to orderly shutdown systems, when possible.
- If a fire or flood occurs, disconnect power if possible and try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
- Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
- Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
- Respond to requests for records via portable phone rather than computer.
- Continue to provide patient charts as requested by physicians or other parties.

Priority Disaster Recovery Tasks:

<u>As applicable, and under appropriate circumstances, all workforce members should</u>:

- Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
- Not permit unauthorized personnel to enter the affected area.
- Determine the extent of the damage and whether additional equipment/supplies are needed.
- Determine how long it will be before service can be restored, and notify departments.
- Replace hardware as necessary to restore service.
- Work with vendors as necessary to ensure that support is given to restore service.

- Notify insurance carriers.
- Retrieve and upload backup files if necessary to restore service.
- Air-dry floppy disks, if any, using a hair dryer on "air," not "heat." When dry, copy disk.
- For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
- Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
- Wrap paper records to prevent them from sticking together. Label the wrapped records.
- Contact fire, water, and storm damage restoration company. Contract for services as needed.
- Reconstruct/reacquire documents from the following:
    - Dictation system.
    - Word processing system.
    - Computer system.
    - Holders of document copies.
- Move records and equipment back to home location.
- Catch up on filing.
- Ensure that backup procedures are followed.
- Document data that cannot be recovered in patient record.
- Meet with management and staff to identify opportunities for improvement.

Additional Disaster Recovery Tasks:

The following tasks must be assigned to specific persons or positions:

- ❑ Determine whether additional equipment and supplies are needed.
- ❑ Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- ❑ If necessary, check with other vendors to see whether they can provide faster delivery.
- ❑ Rush order any supplies and equipment necessary.
- ❑ Notify personnel that an alternate site will be necessary and where it is located.
- ❑ Coordinate moving equipment and support personnel to the alternate site.
- ❑ Bring recovery materials from offsite storage to the alternate site.
- ❑ As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- ❑ Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
- ❑ Prepare backup materials and return them to the offsite storage area.
- ❑ Set up operations at the alternate site if necessary.
- ❑ Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- ❑ Ensure that periodic backup procedures are followed according to our Data Backup Policy.
- ❑ Plan to phase in all critical support.
- ❑ Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- ❑ Coordinate with administration and others for continuing support and ultimate restoration of normal operations.