HIPAA-24 Data Backup and Storage Policy

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

Scope of Policy

This policy governs Data Backups and Storage 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 data backups and storage, in accordance with the requirements at § 164.308(a)(7) and § 164.310(d)(1-2).
- The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- Timely access to health information is crucial to providing high quality health care, and to our business operations.
- Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- It is the Policy of **TCS** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
- This policy includes creating retrievable, exact copies of electronic protected health information, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.
- All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times. This shall include an understanding of the organization's **Recovery Time Objectives** (amount of time to recover data) and **Recovery Point Objective** (amount of data that would be lost)
- Data backup jobs and retention policies will be implemented in accordance with the Document/Data Retention Policy and reviewed periodically to ensure compliance.

Procedures

- **TCS** will back up all such data automatically using an appropriate commercial backup solution based on backup policies which support established Recovery Point Objectives and data retention schedule.
- The Network System Administrator is responsible for performing daily backups on **TCS**'s network, including shared drives containing application data, patient information, financial data, and crucial system information

- ❑ If a Disk-to-Disk Backup solution is utilized, such backup data will be securely replicated to a secured off-site location and maintained in an encrypted status by a responsible organization who shall execute a HIPAA Business Associate Agreement**.** *If a local copy of backup data is maintained on site it will also be encrypted.* If a backup solution using removal backup media is utilized, such media shall be encrypted and stored in a secured off-site location. The media storage vault shall meet fire and disaster standards for such backup media and will be kept locked at all times. Only the organization's authorized HIPAA officers, the network system administrator, and the Executive Director's designees shall have access to the media storage vault. In the event that the off-site secured media vault is not available or properly functioning, the, network system administrator, or Executive Director's designees will remove onsite backup media to a secured offsite location until the media vault becomes available.
- ❑ The network system administrator or other designated individuals shall validate the daily backup jobs, will generate daily reports and maintain such reports for a minimum of 30 days.
- ❑ Any errors will be acted upon immediately. Responsible personnel will use contracted technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ The Network System Administrator is responsible for periodically testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least quarterly and more often if necessary to ensure data restores are sufficient to maintain data integrity, availability, and confidentiality.
- ❑ Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ All personnel who detect or suspect a data backup problem should immediately report the same to the Network System Administrator. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.