Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Contingency Plan*

HIPAA Regulation:

• *Contingency plan*	§164.308(a)(7)	required
• *Data backup plan*	§164.308(a)(7)	required
• *Disaster recovery plan*	§164.308(a)(7)	required
• *Emergency mode operation plan*	§164.308(a)(7)	required
• *Testing and revision procedures*	§164.308(a)(7)	addressable
• *Applications and data criticality analysis*	§164.308(a)(7)	addressable
• *Contingency operations*	§164.308(a)(7)	required

Policy Purpose:

The purpose of this policy is to establish rules to protect the availability, integrity, and security of electronic protected health information (EPHI) while continuing business without the normal resources of the organization.

Policy Description:

Saratoga Bridges shall have documented procedures for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure, and natural disaster) when any system that contains EPHI is affected, including:

- Applications and Data Criticality Analysis
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan

Each of the following plans shall be evaluated and periodically updated as business needs and technology requirements change.

Applications and Data Criticality Analysis

There shall be periodic assessment of the relative criticality of applications and data that contain EPHI for the purposes of maintaining a current Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan.

Saratoga Bridges shall identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact.

Data Backup Plan

All EPHI shall be stored on network servers in order for it to be automatically backed up by the system.

EPHI shall not be saved on the local (C:) drive of any workstation.

EPHI stored on portable media shall be saved to the network to ensure backup of the EPHI.

IT support shall establish and implement a Data Backup Plan that, at a minimum, includes daily backups of user-level and system-level information and weekly backups that are stored securely offsite.

The Data Backup Plan shall apply to all files that may contain EPHI.

The Data Backup Plan shall require that all media used for backing up EPHI be stored in a physically secure environment.

Data backup procedures outlined in the Data Backup Plan shall be tested on at least an annual basis to ensure that copies of EPHI can be retrieved and made available.

Disaster Recovery Plan

To ensure that HIPAA covered components can recover from the loss of data due to an emergency or disaster such as fire, vandalism, system failure, or natural disaster affecting systems containing EPHI, IT support shall establish and implement a Disaster Recovery Plan for restoring or recovering loss of EPHI and the systems needed to make that EPHI available in a timely manner.

The Disaster Recovery Plan shall be documented and available to the assigned personnel, who shall be trained to implement the Disaster Recovery Plan.

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.

Emergency Mode Operation Plan

Saratoga Bridges shall document and implement procedures to enable continuation of critical business processes for the protection of EPHI while operating in emergency mode. Emergency mode operation must include processes to protect the security of EPHI during and immediately after a crisis.

Emergency mode operation procedures outlined in the Emergency Mode Operation Plan shall be tested periodically.

Policy Responsibilities:

Manager and Supervisor Responsibilities

1. Develop and document an Emergency Operations Mode Plan for their units that include appropriate procedures for their workforce.
2. Annually ensure that appropriate emergency operations and disaster recovery procedures are in place.
3. Periodically test their Emergency Operations Mode Plan.
4. Ensure that workforce members save all EPHI on network drives and not on the local drive (C:) of their workstation.

IT Support Responsibilities

1. Establish, implement, and document the Data Backup Plan for EPHI that is used.
2. Annually test the EPHI backups to ensure that exact copies of EPHI can be retrieved.
3. Document and maintain a Disaster Recovery Plan to restore the EPHI applications and data that is needed for the HIPAA covered components to continue their critical business functions in a disaster.
4. Periodically test the documented disaster recovery procedures to ensure that EPHI data and systems can be restored.