Policy Title: Disaster Recovery Plan			
Department Responsible: THN Compliance and Privacy	**Policy Number:** THN-CP-112-0919-Disaster Recovery Plan	**THN's Effective Date:** September 30,2019	**Next Review/Revision Date:** September 30, 2020
Title of Person Responsible: THN Compliance Officer	**THN Approval Council:** Board of Managers	**Date Approved**: September 30, 2019	**Revision Approval Council:**

PURPOSE:

Triad HealthCare Network has developed policies and procedures to assist the company in recovery from to its normal operational state following a disaster.

DEFINITIONS:

Term	Definition

POLICY:

Triad HealthCare Network defines a disaster as any event that affects its information systems and, as a result, substantially interferes with the operations of its business. Examples are fire, flood, hardware failure of critical elements (i.e., server), software failures, theft, chemical/radiation hazard, and sabotage. Triad HealthCare Network's definition of recovering from a disaster is taking all the actions needed to restore the systems to their normal operational state.

PROCEDURE:

A. Triad HealthCare Network will take the following steps in preparation to perform a disaster recovery:
    a. Triad HealthCare Network will train its workforce to recognize and report a disaster.

B. Triad HealthCare Network will organize its workforce responsibilities during a recovery so that the company is not dependent on only one person for any critical step.

C. Triad HealthCare Network workforce members will report disasters to the Privacy & Security Officer. The Privacy & Security Officer will then make the formal determination as to whether or not to classify the event as a disaster.

D. Triad HealthCare Network will store paper backup copies of key disaster-related documents in an offsite location. These documents will include a list of support contacts – vendor, reseller, and/or support group contact information for all of its software and hardware.

E. Triad HealthCare Network will keep a detailed checklist for each IT asset, such as the server, PCs, router, network switch, databases, and software programs containing tasks that must be completed to recover that asset. The list will include key data about the asset, including the party responsible for the diagnosis and, if needed, repair, replacement, and/or rebuilding of a device.

F. Triad HealthCare Network will have current copies of its system data and software available at an offsite location, as specified in its Data Backup Plan.

G. Once a disaster has been certified, Triad HealthCare Network will:
   a. Use the Privacy & Security Officer or designee to facilitate the recovery. The facilitator will direct the recovery process, coordination, and communication of the actions of the various parties that are involved in the recovery.
   b. Determine which devices/software (i.e., server, PCs, power units, A/C units) are not functioning normally, conferring with the appropriate staff, vendors, and other support personnel to make this determination. When in doubt about the status of the device, Triad HealthCare Network will depend on the recovery responsible party to make this determination.
   c. Contact the appropriate recovery responsible parties for the devices/software to be recovered. Guidance and other recovery activities from these parties are key contributors to the recovery process.
   d. After all of the non-functioning assets have been restored, follow the instructions of the designated workforce member as to what to do when the system is again available.

REFERENCE DOCUMENTS/LINKS:

COMMITTEE APPROVAL:

PREVIOUS REVISION/REVIEW DATES:

Date	Reviewed	Revised	Notes