	Information Security Policies and Procedures	No. COMP-Sec 6.0.0
	Title: CONTINGENCY PLANNING POLICY	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 01/09/01

Contingency Planning Policy

I. SCOPE

This policy applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This policy applies to all Tenet HealthCare Corporation divisions, facilities and related departments.

II. PURPOSE

The Contingency Planning Policy authorizes facility management to develop, implement and maintain a comprehensive Contingency Planning Program. The intent of this program is to protect the safety of our workforce members and mitigate potential risk(s) that could materially affect the ability of the facility to remain a going concern. The major focus of the documents described in this policy and the related Standards and Procedures is to plan for the identification, protection, and recovery of critical information assets in the event of a disaster. These documents shall serve as a supplement to the Facility’s Disaster Recovery Plan.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception will be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. POLICY


The Contingency Planning Program components include, but are not limited to:

A. Contingency Plan

Each facility is responsible for developing, implementing and maintaining a comprehensive Contingency Plan. The Contingency Plan shall encompass the DCA, DBP, BCP, ERP, and DRP.

B. Data Criticality Analysis (“DCA”)

Each facility is responsible for conducting a DCA to identify essential business functions that must be recovered in the event of a disaster for the facility to remain a going concern. The DCA is used to identify mission critical applications and data sets and determine the recovery priority of this information in the event of a loss of availability. The DCA may be used in conjunction with cost-benefit analyses to determine recovery strategies and to help target information that shall be backed up and relied upon in the event of an emergency.

	Information Security Policies and Procedures	No. COMP-Sec 6.0.0
	Title: CONTINGENCY PLANNING POLICY	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 01/09/01

C. Data Backup Plan (“DBP”)

Information essential to the facility shall be backed up, stored in a secured facility away from the primary source location and be made available upon recall for recovery purposes (tape, compact disc, microfiche, film, video, paper, etc.). Each facility is responsible for developing, implementing and maintaining a Data Backup Plan to document this process.

D. Emergency Response Plan (“ERP”)

Each facility is responsible for developing, implementing and maintaining an ERP that lists critical resources and procedures to be followed beginning at the onset of a potential emergency through the time a disaster declaration has been made.

E. Business Continuity Plan (“BCP”)

Each facility is responsible for developing, implementing and maintaining a BCP that outlines how the facility should continue to conduct critical business operations while recovering from an emergency and/or declared disaster.

F. Disaster Recovery Plan (“DRP”)

Documented procedures to restore and recover the facility’s critical information assets shall be developed, implemented and maintained for each facility. The DRP shall list resources and recovery procedures for critical outsourced systems as well as critical systems provided and/or managed by Tenet.


G. Contingency Testing Plan (“CTP”)

Documented processes to be used when testing the facility’s entire Contingency Planning Program, including the BCP and the DRP.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Information Access Control Standard No. 3.1.0.
- Contingency Planning Standard No. 6.1.0.
- Contingency Planning Procedure No. 6.1.1.

	Information Security Policies and Procedures	No. COMP-Sec 6.0.0
	Title: CONTINGENCY PLANNING POLICY	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 01/09/01

- Asset Access Control Standard No. 8.1.0.
- Backup Procedure No. 8.2.3.
- Site Specific Contingency Plans.