	Information Security Policies and Procedures	No. COMP-Sec 7.0.0
	Title: SECURITY ADMINISTRATION POLICY	Page: 1 of 3
		Revised Date: 12/22/04
		Original Date: 03/09/01

Security Administration 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 information assets and facility management.

II. PURPOSE

Provide guidance to management on certain administrative functions and to identify those responsible for controlling and monitoring those functions. Tenet’s Information Security Policies and Procedures require certain administrative functions to ensure ongoing guarding of data integrity, confidentiality and availability.

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 administrative procedures discussed below shall be followed to ensure continued protection of data and management of User conduct in relation to the protection of data.

A. Evaluation

An internal evaluation of a facility’s compliance with Tenet’s Information Security Policies and Procedures shall be conducted by the Corporate Privacy/Security Office to establish the extent to which each facility complies. This evaluation shall include a review process that establishes the extent to which a particular computer system or network design meets security requirements. The evaluation will address both technical and non-technical components of security.

B. Privacy/Security Vulnerability Reviews

After the initial evaluation is conducted, privacy/security vulnerability reviews shall be performed at each facility as required, with the goal of reviewing each facility bi-annually. The Corporate Privacy/Security Office has the right to prioritize reviews based on risk analyses, and shall conduct these reviews in accordance with their audit program. Facility management shall be responsible for ensuring that all vulnerabilities identified during the review are addressed.

	Information Security Policies and Procedures	No. COMP-Sec 7.0.0
	Title: SECURITY ADMINISTRATION POLICY	Page: 2 of 3
		Revised Date: 12/22/04
		Original Date: 03/09/01

C. Privacy/Security Self-Evaluations

Self-evaluations shall be performed at each facility at the direction of the Corporate Privacy/Security Office, whenever significant changes are made to information assets, or otherwise on an as needed basis. The Corporate Privacy/Security Office will make resources used in the privacy/security vulnerability review process available to all hospitals for use in self-evaluations. The Corporate Privacy/Security Office shall be informed when a self-evaluation is complete and shall perform accreditations as necessary. Management of the evaluation processes will be shared between facility management and the Corporate Privacy/Security Office.


D. Training

Education concerning the vulnerabilities of CONFIDENTIAL information and ways to ensure protection of that information will be provided to all Tenet information asset Users. This training shall include:

1. Security awareness training for all information asset Users covering topics such as:
 - a) Password maintenance and management.
 - b) Monitoring of log-in success or failure.
 - c) Incident reporting.
 - d) Viruses and other malicious software.
 - e) Physical security practices.
2. Security reminders provided to all information asset Users.
 - a) Development of the training material and methods for distribution will be the responsibility of the Corporate Privacy/Security Office.

E. Risk Management

Information security risk management includes risk assessment, risk reduction, and risk level maintenance. Each facility is responsible for performing risk management procedures, including maintaining their Information Security Control Exceptions Book.

	Information Security Policies and Procedures	No. COMP-Sec 7.0.0
	Title: SECURITY ADMINISTRATION POLICY	Page: 3 of 3
		Revised Date: 12/22/04
		Original Date: 03/09/01

The standards of Tenet’s information security risk management process are defined in the Information Security Risk Management Program Standard No. 7.1.0.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following Tenet documents

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0.
- Information Classification Standard No. 2.1.0.
- Information Handling Procedure No. 2.1.1.
- Security Risk Management Standard No. 7.1.0.
- Asset Access Controls Standard No. 8.1.0.
- Logging and Auditing Procedure No. 8.2.2.
- Tenet Administrative Policies and Procedures No. 3.3 “Facility Risk Management Reporting Requirements”.
- Tenet Human Resources Policies and Procedures No. 513 “Workplace Monitoring”.