	Information Security Policies and Procedures	No. COMP-Sec 4.1.0
	Title: SANCTIONS STANDARD	Page: 1 of 2
		Revised Date: 12/22/04
		Original Date: 10/17/00

Sanctions Standard

I. SCOPE

This standard 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 standard applies to all Tenet information assets and information asset Users.

II. PURPOSE

To provide notification and clarification of the penalties that may result from failure to comply with the Tenet Information Security policies and procedures.

III. STANDARD

The Tenet Information Security Policies and Procedures require all Users of Tenet’s information assets to adhere to those policies, standards and procedures. Violations of those Policies are grounds for corrective action up to and including professional discipline, termination, and civil or criminal prosecution.

A. Employee Performance Management


The Tenet Employee Manual outlines a positive performance management and progressive corrective action approach used whenever possible to motivate employees’ participation in the resolution of situations where performance does not meet company expectations and standards. Breaches of confidentiality of health information or other violations of the Tenet Information Security Policies and Procedures expose the employee to the full range of options incorporated in the Performance Management Policy as well as the possibility of professional discipline, and civil or criminal prosecution.

B. Other Sanctions

At any point in these processes, access to Tenet’s information assets may be restricted or removed at the discretion of facility management.

Facility management shall include a provision in contracts with third parties, to allow for initiation of contract penalties or termination of contracts for violation of information security policies.

Violation of Tenet’s Information Security Policies and Procedures or breach of confidentiality of health information may constitute a breach of professional ethics.

	Information Security Policies and Procedures	No. COMP-Sec 4.1.0
	Title: SANCTIONS STANDARD	Page: 2 of 2
		Revised Date: 12/22/04
		Original Date: 10/17/00

Violations may be reported to the applicable regulatory, licensure or accreditation organization. Facility management shall cooperate with any professional investigation or disciplinary proceeding.

Violation of Tenet’s Information Security Policies and Procedures or breach of confidentiality of health information may constitute a civil or criminal offense. Facility management may provide information regarding the violation to law enforcement personnel and cooperate with any law enforcement investigation, as required by law.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Information Access Control Standard No. 3.1.0.
- Information Security Awareness Training Standard No. 3.2.0.
- Incident Handling Policy No. 4.0.0.
- Incident Response Procedure No. 4.1.1.
- Physical Safeguards for Information Assets Policy No. 5.0.0.
- Tenet Asset Access Controls Standard No. 8.1.0.
- Tenet Administrative Policies and Procedure No. 2.25 “Security Incident Reporting”.
- Tenet Administrative Policies and Procedure No. 2.35 “Information Systems: Sensitivity, Confidentiality, and Appropriate Use”.
- Tenet Human Resources Policies and Procedure No. 401 “Employee Conduct and Work Rules”.
- Tenet Human Resources Policies and Procedure No. 408 “Performance Management”.
- Tenet Employee Handbook.
- Tenet Standards of Conduct.