	Information Security Policies and Procedures	No. COMP-Sec 2.1.0
	Title: INFORMATION CLASSIFICATION STANDARD	Page: 1 of 4
		Revised Date: 12/22/04
		Original Date: 10/09/00

Information Classification 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

Protecting the confidentiality, integrity, and availability of information requires information be identified by level of sensitivity. Special handling consideration is given to information depending on the level of sensitivity. This document outlines the enterprise-wide information classification standard. Appropriate information security processes and mechanisms can then be applied to adequately protect each level of information.

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


III. STANDARD

There are three sensitivity classifications for information with separate handling requirements: *CONFIDENTIAL*, *PROPRIETARY*, and *PUBLIC*. These classifications are defined as follows:

A. *Confidential*

CONFIDENTIAL refers to the most sensitive business information intended strictly for use within and between Tenet and authorized third parties. Unauthorized disclosure of this information could adversely impact Tenet, its stockholders, its business partners, its patients and/or its customers. Examples of this information include, but are not limited to:

- a) Protected health information (PHI)
- b) Electronic protected health information (ePHI)
- c) Employee personnel files
- d) Payroll information

	Information Security Policies and Procedures	No. COMP-Sec 2.1.0
	Title: INFORMATION CLASSIFICATION STANDARD	Page: 2 of 4
		Revised Date: 12/22/04
		Original Date: 10/09/00

- e) Business strategies
- f) Quality Assurance documentation
- g) Clinical research documentation
- h) Attorney-client privileged documents
- i) Attorney work products
- j) Trade secrets

PHI is a particular type of *CONFIDENTIAL* Information. It includes information identifiable to a particular patient and includes the patient's medical history, diagnosis, treatment, prognosis, or information related to billing or payment whether in hardcopy or electronic form.

B. Proprietary


PROPRIETARY refers to all information that is not *CONFIDENTIAL* or *PUBLIC*. This information is intended for use within Tenet unless authorized for additional distribution. Examples of this information include:

- a) Internal telephone numbers
- b) Financial information
- c) Policies and procedures
- d) eTenet Intranet website content

C. Public

PUBLIC refers to all information that has been released to the public by Tenet. Examples of this information include:

- a) Job postings
- b) Annual reports

	Information Security Policies and Procedures	No. COMP-Sec 2.1.0
	Title: INFORMATION CLASSIFICATION STANDARD	Page: 3 of 4
		Revised Date: 12/22/04
		Original Date: 10/09/00

c) Facility internet website content

Refer to the Administrative Policies and Procedures No. 1.9, “Public Release of Information” for further information.

D. Responsibility for Assigning Information Classification

Information Owners determine the sensitivity classification of information. The classification shall be based on the classification definitions provided herein. Facility Management shall instruct Information Owners, as needed, on the proper assignment of information classification levels.


E. Descriptive Suffixes

Suffixes such as "*Patient Record*", "*Attorney/Client Privileged*", "*Financial*", "*Draft*" or other descriptive terms may be used after the term *CONFIDENTIAL* or *PROPRIETARY* (separated by a hyphen) to further restrict information to particular groups or Users.

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 Handling Procedure No. 2.1.1.
- User Security Policy No. 3.0.0.
- Information Access Control Standard No. 3.1.0.
- Access Request and Modification Procedure No. 3.1.1.
- Access Termination Procedure No. 3.1.2.
- Security Administration Policy No. 7.0.0.
- Technical Security Management Policy No. 8.0.0.

	Information Security Policies and Procedures	No. COMP-Sec 2.1.0
	Title: INFORMATION CLASSIFICATION STANDARD	Page: 4 of 4
		Revised Date: 12/22/04
		Original Date: 10/09/00

- Asset Access Controls Standard No. 8.1.0.
- Information Asset Administration Standard No. 8.2.0.
- Change Control Procedure No. 8.2.1.
- Network Security Administration Standard No. 8.3.0.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.
- Tenet Administrative Policies and Procedures No. 1.1 “Access to Patient and Medical/Professional Staff Records”.
- Tenet Administrative Policies and Procedures No. 1.9 “Public Release of Information”.
- Tenet Administrative Policies and Procedures No. 1.11 “Records Management”.
- Tenet Human Resources Policies and Procedures No. 032-f “Access to Personnel Records”.
- Tenet Human Resources Policies and Procedures No. 304 “Contacts with Government Regulatory Agencies”.
- Tenet Human Resources Policies and Procedures No. 306 “Records Retention”.
- Tenet Human Resources Policies and Procedures No. 513 “Workplace Monitoring”.
- Tenet Privacy Policies and Procedures.