	Information Security Policies and Procedures	No. COMP-Sec 2.0.0
	Title: RECORD PROCESSING POLICY	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 10/09/00

Record Processing 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 information asset Users.

II. PURPOSE

Provide standards, procedures and guidelines for processing records including the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of electronic and paper documents containing PHI and *CONFIDENTIAL* or *PROPRIETARY* information. Information is an important corporate asset that requires protection from loss, misuse, theft, and unauthorized revision while the information is in the possession of the corporation.

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. POLICY

It is the policy of Tenet to preserve the confidentiality, integrity, and availability of information obtained, created, processed, stored, transmitted and/or disposed in the course of performing business and patient care processes. Measures to protect this information are established in accordance with the level of sensitivity of the information and appropriate risk management practices.


A. Information is *CONFIDENTIAL*, *PROPRIETARY*, or *PUBLIC*

All data within the Tenet information assets, generated by the Tenet information assets, or in anyway related to Tenet information assets, is considered *CONFIDENTIAL*, *PROPRIETARY*, or *PUBLIC*.

See the Information Classification Standard No. 2.1.0 for definitions.

B. Record Processing

Protected health information (PHI) and other *CONFIDENTIAL* or *PROPRIETARY* information, whether in electronic or paper format, shall be protected from unauthorized disclosure throughout the processes of routine and non-routine receipt, creation, manipulation, storage, dissemination, transmission, and/or disposal. It is expected all

	Information Security Policies and Procedures	No. COMP-Sec 2.0.0
	Title: RECORD PROCESSING POLICY	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 10/09/00

Users will maintain the confidentiality of this information. Tenet information asset Users will be provided access to *CONFIDENTIAL* and *PROPRIETARY* information based on their need to know and job requirements.

- a) Each User of electronic protected health information (ePHI) must have an individual UserID and confidential password for accessing that information.
- b) Access to PHI shall be managed through active application of system controls, physical controls, and auditing. For additional information on this topic, refer to the Information Handling Procedure No. 2.1.1.

1. *ROUTINE AND NON-ROUTINE RECEIPT AND CREATION*

All PHI created or received by Users of Tenet information assets is the property of Tenet. Tenet facility management shall define the process for receiving PHI and incorporating it into Tenet records. These processes shall include steps for acknowledgment and verification of the information received and include all formats such as faxed, telephoned, transcribed, and e-mailed information.

Tenet facility records management personnel shall develop processes and guidelines for creation of PHI records that comply with all policies, laws and regulations.

2. *ROUTINE AND NON-ROUTINE MANIPULATION*


Tenet facility management shall define the procedures governing the movement, assembly and maintenance of PHI.

Tenet facility management or corporate information owners shall define procedures governing the movement, assembly, and maintenance of other *CONFIDENTIAL* or *PROPRIETARY* information.

3. *STORAGE*

PHI shall be archived and maintained, whether within the facility or at off-site locations, as identified in law, accreditation and professional practice standards.

Tenet facility management shall define standards and procedures for their local environment that meet the requirements of legal, regulatory, and accrediting agencies for off-site storage of *CONFIDENTIAL* or *PROPRIETARY* information.

	Information Security Policies and Procedures	No. COMP-Sec 2.0.0
	Title: RECORD PROCESSING POLICY	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 10/09/00

For more information on this topic, refer to Tenet’s Administrative Policies and Procedures No. 1.11 “Records Management”.

4. ROUTINE AND NON-ROUTINE DISSEMINATION

See Tenet’s Privacy Policies for specific requirements related to uses and disclosures of PHI.

- a) Dissemination refers to the use and disclosure of information.
- b) PHI shall not be disclosed unless authorized by law, the patient, or when a defined medical emergency exists.
- c) Tenet facility management shall define rules of distribution of CONFIDENTIAL and PROPRIETARY information and review those rules routinely to validate the application of need to know principles.
- d) Requests for release of PHI from third parties shall be governed by applicable laws and shall be referred to the Facility’s Health Information Management Department or the Information Owner (See duties in the Access Request and Modification Procedure No. 3.1.1 of the Information Security Policies and Procedures).

5. TRANSMISSION

Transmission of information is the transfer of data between applications, systems, companies, or personnel. It is Tenet’s policy to protect CONFIDENTIAL and PROPRIETARY information against unauthorized access, inadvertent disclosure, and loss of data integrity during transmission.

For more information on this topic, refer to the Asset Access Control Standard No. 8.1.0 and the Transmission Security Procedure No. 8.3.6.


6. DISPOSAL

CONFIDENTIAL and PROPRIETARY information shall be disposed according to Tenet’s Records Management Policy and Procedure.


IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following Tenet documents:

Tenet Healthcare Corporation

	Information Security Policies and Procedures	No. COMP-Sec 2.0.0
	Title: RECORD PROCESSING POLICY	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 10/09/00

- Corporate Information Security Policy No. 1.0.0.
- Information Classification Standard No. 2.1.0.
- 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.
- 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.
- Transmission Security Procedure No. 8.3.6.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.
- 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”.

	Information Security Policies and Procedures	No. COMP-Sec 2.0.0
	Title: RECORD PROCESSING POLICY	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 10/09/00

- 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.