	Information Security Policies and Procedures	No. COMP-Sec 5.0.0
	Title: PHYSICAL SAFEGUARDS FOR INFORMATION ASSETS POLICY	Page: 1 of 2
		Revised Date: 12/22/04
		Original Date: 01/09/01

Physical Safeguards for Information Assets 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 members of the Tenet Workforce.

II. PURPOSE

Provide overall direction for the application of physical security principals to ensure the protection of Tenet information assets. Information assets shall be protected from physical threats including damage from human, natural or accidental events.

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

Physical security can be broken down into two elements, site physical security and information asset physical security. The Physical Safeguards for Information Assets Policy No. 5.0.0 shall be reviewed when establishing a facility’s Information Asset Physical Security policies and procedures for the protection of information and information assets.

A. Individual Access

Physical access to Tenet information assets is granted on a need-to-know basis.


B. Healthcare Specific Concerns

Hospitals, clinics and offices maintain open public access. Physical security shall be addressed in such a way that risk to information assets is minimized.

C. Responsibilities

Management will be responsible for:

- a) Developing, implementing, maintaining and enforcing information asset physical security policies.

	Information Security Policies and Procedures	No. COMP-Sec 5.0.0
	Title: PHYSICAL SAFEGUARDS FOR INFORMATION ASSETS POLICY	Page: 2 of 2
		Revised Date: 12/22/04
		Original Date: 01/09/01

- b) Ensuring policies and procedures are tested and reviewed at least annually. Results of testing and review shall be used to make changes to policies and procedures as needed.
- c) Documenting exceptions to policies and procedures and identifying compensating controls where exceptions are made.

Remote users, such as telecommuters or small offices shall comply with the items that are applicable to their situations.

D. Maintenance Records

Records of maintenance performed on information asset physical security safeguards (i.e. hardware, software, walls, doors, locks) shall be kept. These records shall include:

- a) Documentation of repairs;
- b) Documentation of installations; and
- c) Documentation of modifications (including lock/key changes).

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following Tenet documents:

- Corporate Information Security Policy No. 1.0.0.
- Information Access Control Standard No. 3.1.0.
- Sanction Standard No. 4.1.0.
- Information Asset Secured Area Protection Standard No. 5.1.0.
- Information Asset Open Area Protection Standard No. 5.2.0.
- Asset Access Control Standard No. 8.1.0.
- Site Specific Physical Security Policies.
- Tenet Human Resources Policies & Procedures No. 804 “Security Inspections”.