	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 5.2.0</b>
	<b>Title: INFORMATION ASSET OPEN AREA PROTECTION STANDARD</b>	<b>Page: 1 of 3</b>
		<b>Revised Date: 06/13/06</b>
		<b>Original Date: 11/03/00</b>

**Information Asset Open Area Protection 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 members of the Tenet Workforce.

**II. PURPOSE**

Provide guidance on the precautions Users shall take to protect the confidentiality, availability, and integrity of Tenet’s information assets located in unsecured areas. Tenet information assets cannot always be locked in Data Centers or other secure and protected areas. These assets may be located in offices, cubicles, nurse stations, or at home for telecommuters. Precautions shall be taken when information assets are located outside protected areas.

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. STANDARD**

When possible, access to every office or work area containing *CONFIDENTIAL* information shall be physically restricted. In areas that cannot be secured, alternate compensating controls shall be implemented.

A. Unsecurable Areas

Special precautions shall be taken within unsecurable areas to protect *CONFIDENTIAL* information and information assets capable of accessing *CONFIDENTIAL* information. The following shall be considered by site management when assessing unsecurable areas:

- a) Store *CONFIDENTIAL* information in a secured enclosure (e.g. locked drawers or cabinets) when not attended by a member of the workforce; or
- b) Store *CONFIDENTIAL* information in a separate lockable room (e.g. medication storage behind nurse station, supply storeroom) when not attended by a member of the workforce;
- c) Secure information assets using adequate access controls. Laptop computers

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 5.2.0</b>
	<b>Title: INFORMATION ASSET OPEN AREA PROTECTION STANDARD</b>	<b>Page: 2 of 3</b>
		<b>Revised Date: 06/13/06</b>
		<b>Original Date: 11/03/00</b>

and other portable information assets that store confidential information should be stored in a secured enclosure (e.g. locked drawers or cabinets) when not attended by a member of the workforce; and


- d) Take reasonable precautions to protect an individual’s privacy when engaging in common health care practices. These practices can include maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g. “high fall risk”) at patient bedside or at the doors of hospital rooms. Possible safeguards may include reasonably limiting access to the area, ensuring that the area is supervised, placing patient charts in their holders with identifying information covered or facing the wall or counter, or limiting patient names to just first name and last initial or first initial and last name.

**B. Information Visibility**

The display screens for all PCs, monitors or any other device that displays confidential information shall not be oriented so that unauthorized individuals may view the information. This includes through a window, across a counter or desk, from a waiting area or by individuals passing by in a walkway, hall or corridor. See the Information Handling Procedure No. 2.1.1 for further details on protecting information.

**C. Power Protection**

- a) Tenet information assets that are critical to the operation of business shall be attached to an uninterruptible power supply (UPS). This includes:
  - (i) The facility’s main UPS system; and
  - (ii) Commercially available stand alone UPS systems.
- b) Information assets that are on a stand-alone UPS shall be configured to monitor the UPS for power availability and shut down accordingly.
- c) All stand-alone computing assets (PCs, workstations, terminals, routers, or other computing assets) that are not directly hooked to a UPS system should have a power spike suppression system between the asset and the power source. These suppression devices shall be of sufficient capacity to protect the equipment attached.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 5.2.0</b>
	<b>Title:</b> <b>INFORMATION ASSET OPEN AREA PROTECTION STANDARD</b>	<b>Page: 3 of 3</b>
		<b>Revised Date: 06/13/06</b>
		<b>Original Date: 11/03/00</b>

D. Theft Protection

It is recommended that all stand-alone information assets have anti-theft devices attached to protect the assets from theft. This includes, but is not limited to:

- a) Cable Locks;
- b) Permanent (bolted) mounting; and
- c) Case Locks.

**IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following Tenet documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0 and subordinate Standards and Procedures.
- Physical Safeguards for Information Assets Policy 5.0.0.
- Information Asset Secured Area Protection Standard No. 5.1.0.
- Tenet Corporate Physical Security Policy.