	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 3.2.0</b>
	<b>Title: INFORMATION SECURITY AWARENESS STANDARD</b>	<b>Page: 1 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 10/27/00</b>

**Information Security Awareness 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 Covered Entity’s workforce, and other individuals and organizations as applicable.

**II. PURPOSE**

Establish the major elements of the Tenet Information Security Awareness Program. The Information Security Awareness Program is designed to educate and reinforce User awareness of information security responsibilities and practices.

**III. STANDARD**

The following are individual programs that, when combined together, form a complete and effective information security awareness program. Vendors and other third parties shall be made aware of applicable Tenet Information Security Policies and Procedures in their respective business associate agreements or through other means as determined by Tenet.

A. Orientation Training


All Users new to Tenet information assets shall attend an “Orientation” class in accordance with Human Resources Policies and Procedures No. 307-F “Employee Orientation”.

1. TRAINING REQUIREMENTS

Orientation training shall be provided within 30 days of the workforce member’s initial employment (or sooner). Information Security issues shall be addressed in that class.

2. TRAINING CONTENT

The Tenet Information Security Awareness Program shall use the Information Security Policies, Standards and Procedures to raise the level of awareness of each User of Tenet information assets at orientation. Training topics shall include:

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 3.2.0</b>
	<b>Title: INFORMATION SECURITY AWARENESS STANDARD</b>	<b>Page: 2 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 10/27/00</b>

- a) Password use, maintenance, and protection;
- b) Malicious software threat protection, prevention, and response;
- c) Incident reporting and response;
- d) Monitoring and awareness of login failures;
- e) Software licensing rules;
- f) Appropriate use and protection of *CONFIDENTIAL* and *PROPRIETARY* information; and
- g) Physical security mechanisms for protecting information assets.

B. General Information Security Training


Tenet shall establish procedures to train members of its workforce in an ongoing, consistent manner.

1. TRAINING REQUIREMENTS

Training shall be provided according to the following procedures:

- a) Current Members of the Workforce. Training will be provided to all current workforce members no later than April 21, 2005, which is the date that compliance is required with the Security Rule. All Workforce members are required to participate in one or more of the training programs listed below.
- b) New Members of the Workforce. A person who joins the workforce after April 21, 2005, will be trained concerning Tenet's Information Security Policies and Procedures as part of the person's orientation or otherwise within 30 days after the date that the person joins the Workforce.
- c) Changes in Policies and Procedures Regarding Information Security. Each workforce member whose functions are affected by a material change in these Information Security Policies and Procedures will be provided additional training within 30 days after the effective date of the change.

2. TRAINING MATERIALS

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 3.2.0</b>
	<b>Title: INFORMATION SECURITY AWARENESS STANDARD</b>	<b>Page: 3 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 10/27/00</b>

The Corporate Privacy/Security Office will develop/maintain the following training materials:

- a) Online training through .edu;
- b) Powerpoint presentation (paper-based) training; and
- c) Face-to-face training sessions as requested.

All privacy training materials shall be reviewed and approved by the Corporate Privacy/Security Office prior to implementation.

### 3. TRAINING DOCUMENTATION


Training documentation will include the time, date, place and content of each training session, as well as the workforce members who attended each training session. The Corporate Privacy/Security Office will maintain such documentation in Tenet's HIPAA compliance files and make it available for inspection by regulatory authorities, as appropriate.

- a) On-Line Training. Participation in on-line training sessions shall be documented and maintained by Tenet's Corporate Privacy/Security Office. A reporting tool will be available to Education Coordinators and/or requests for compliance reports shall be made via email to [privacysecurityoffice@tenethealth.com](mailto:privacysecurityoffice@tenethealth.com).
- b) Classroom Training. Attendance at classroom training sessions held at individual facilities shall be documented (See form at Addendum A). Original documentation shall be maintained by the Covered Entity's Human Resources Department or Education Department. Copies of the attendance sheets shall be forwarded to Tenet's Privacy/Security Office at least quarterly.

### 4. RECORD RETENTION

Documentation relating to training shall be maintained as follows:

- a) Training attendance documentation for employees shall be maintained for 6 years by the Corporate Privacy/Security Office.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 3.2.0</b>
	<b>Title: INFORMATION SECURITY AWARENESS STANDARD</b>	<b>Page: 4 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 10/27/00</b>

- b) Training attendance documentation for non-employees shall be maintained for 6 years by the facility to which the non-employee reports.
- c) Training materials shall be maintained by the Corporate Privacy/Security Office for 6 years from date of implementation or the date it was last utilized, whichever was latest.

5. NOTIFICATION OF DELINQUENCY

The Corporate Privacy/Security Office will notify facility management (the CFO or designee) quarterly identifying current and new members of the workforce who have not completed training sessions timely. It will be the responsibility of facility management to ensure training is completed timely.


C. Reminders

Facility management shall provide reminders of the importance of information security as appropriate.

**IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0.
- User Security Policy No. 3.0.0.
- Information Access Controls Standard No. 3.1.0.
- Access Request and Modification Procedure No. 3.1.1.
- User Conduct Standard No. 3.3.0.
- Malicious Software Protection Procedure No. 3.3.1.
- Password Use Procedure No. 3.3.2.
- Incident Handling Policy No. 4.0.0.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 3.2.0</b>
	<b>Title:</b> <b>INFORMATION SECURITY AWARENESS STANDARD</b>	<b>Page: 5 of 7</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 10/27/00</b>

- Physical Safeguards for Information Assets Policy No. 5.0.0.
- Contingency Planning Policy No. 6.0.0.
- Security Administration Policy No. 7.0.0.
- Technical Security Management Policy No. 8.0.0.
- Tenet Human Resources Policies and Procedures No. 307-F “Employee Orientation”.



