	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 1 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

Corporate Information Security 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). The Tenet Information Security Policies and Procedures apply to:

- a) All Users of Tenet’s information assets that may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, and business partners (*Users*).
- b) All Users, whether working at Tenet sites, remotely, or in any other situation where Tenet information or information assets are used or accessed.
- c) All Tenet information assets regardless of the controlling facility, department or entity, include, but are not limited to: computers, networks, telephones, magnetic or optical media, and paper; where these information assets are being generated, created, accessed, viewed, processed, stored, used, acquired, purchased, obtained, manipulated, modified, deleted or disposed. Some policies are not relevant for certain types of information assets, so professional judgment should be used during implementation to apply the policies where appropriate.

II. PURPOSE

Tenet Information Security Policies and Procedures have been established to outline Tenet’s directives for information security. These directives include:

- a) Communicating expectations concerning information security to Tenet employees, contractors, consultants, clients, vendors, business partners, and other Users of information and information assets.
- b) Promoting information security awareness.
- c) Establishing responsibility for overseeing information security matters and establishing a mechanism to notify the appropriate personnel in case of an information security incident.
- d) Establishing guidelines to assess security and protection techniques applied to information and information assets.

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 2 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

III. POLICY

This document, along with its subordinate policies, standards, procedures and guidelines, the Information Security Policies and Procedures, establishes uniform policies, responsibilities, and authorities for the implementation of information security at Tenet.


Tenet uses on-line information systems attached to a network of hospitals, clinics, and other facilities to manage business operations and healthcare information. Tenet has a duty to protect the confidentiality, integrity, and availability of medical and business information as indicated or required by best business practices, accepted information security standards, laws, professional ethics and accreditation requirements.

Users of Tenet computing assets or facilities shall not assume their actions are private, privileged or protected. Tenet reserves the right to monitor Users in any manner the company deems appropriate. This may include video, audio or electronic monitoring of activities such as:

- a) Telephone conversations
- b) E-mail content and destinations
- c) Internet access and downloading
- d) Data access
- e) Key strokes
- f) Work habits

Tenet Information Security Policies and Procedures provide direction for:

- a) Protecting Tenet's information and information assets against accidental or deliberate modification or destruction through use of a continuing program of risk assessment and management.
- b) Preventing the unauthorized (accidental or deliberate) disclosure, misuse, or misappropriation of information.
- c) Detecting unauthorized access or misuse of information and information assets.
- d) Performing damage assessments in a timely and accurate manner following the detection of unauthorized disclosure of information, or the unauthorized penetration or misuse of

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 3 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

information assets.


- e) Reporting and correcting vulnerabilities and exposures within Tenet’s information assets.

A. Responsibilities

Responsibility for the content and administration of Information Security Policies and Procedures resides with Tenet’s Privacy/Security Officer. Responsibility for implementing Information Security Policies and Procedures at the facility level resides with the facility Information Security Officer and facility management; provided, however, that Tenet’s Privacy/Security Officer has the overall final responsibility for the security of Tenet’s information assets.

Tenet’s Privacy/Security Officer is responsible for:


- a) Holding the overall final responsibility for the security of Tenet’s information assets.
- b) Working with Tenet senior management to develop policies and procedures, standards, and guidelines that contribute to the realization of the Tenet’s goals and objectives for information, information systems, and information security management.
- c) Working with system administrators, managers, Users and clients to ensure Tenet’s information assets achieve and maintain compliance with Information Security Policies and Procedures, other applicable industry standards, and legal obligations.
- d) Coordinating and directing specific actions to provide a secure and stable information systems environment consistent with Tenet’s goals and objectives.
- e) Collaborating with the Audit Services Department to assure the performance of audits of information systems and information system User activity.
- f) Collaborating with corporate and facility management on the development and implementation of ongoing training and awareness programs for Tenet’s information asset Users.
- g) Collaborating with corporate and facility management on the development of recommendations to improve information security throughout the organization.

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 4 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

- h) Collaborating with Corporate and facility Information Systems resources to investigate information security incidents.
- i) Collaborating with Corporate and facility Compliance resources to address congruent management of Tenet’s Information Security Policies and Procedures and Tenet’s Privacy Policies and Procedures.
- j) Reviewing and reporting the occurrence of information security incidents and remediation efforts.
- k) Overseeing the measurement and reporting of the information security program’s function and outcomes.

Each facility’s Information Security Officer is responsible for:

- a) Working with Tenet’s Privacy/Security Officer to develop and/or adopt policies and procedures, standards, and guidelines that contribute to the realization of the facility’s goals and objectives for information, information systems, and information security management.
- b) Working with system administrators, managers, Users and clients to ensure the facility’s information assets achieve and maintain compliance with Information Security Policies and Procedures, other applicable industry standards, and legal obligations.
- c) Coordinating and directing specific actions to provide a secure and stable information systems environment consistent with the facility’s goals and objectives.
- d) Collaborating with system administrators to assure the performance of audits of information systems and information system User activity.
- e) Collaborating with corporate and facility management on the development and implementation of ongoing training and awareness programs for the facility’s information asset Users.
- f) Collaborating with corporate and facility management on the development of recommendations to improve information security throughout the facility.
- g) Collaborating with the Corporate Privacy/Security Office, the Hospital Compliance Officer, and facility Information Systems resources to investigate

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 5 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

information security incidents.

- h) Reviewing and reporting the occurrence of information security incidents and remediation efforts.
- i) Ensure systems comply with Information Security Policies and Procedures.
- j) Assess, document, and obtain approvals for exceptions to the Information Security Policies and Procedures.

1. Other Responsibilities


a) *Information Asset Owners*

Information Asset Owner responsibilities may be delegated by facility management or the Information Asset Owner. The following bullets outline the major duties of an Information Asset Owner:


- (i) Develop written statements indicating the individuals who have been granted authority to originate, modify, or delete specific types of information found in the assets under the owner's purview.
- (ii) Determine the appropriate classification and criticality rating for the data.
- (iii) Determine who will be permitted access to the information. The owner may delegate the responsibility for granting or denying access to the asset to subordinates or peers, but not to the request processing entity unless the asset is considered open or public.
- (iv) Determine the purposes for which information assets will be used.
- (v) Work with facility management and the Corporate Privacy/Security Office to review access to their assets on at least an annual basis.

b) *Information Asset System Administrator or Security Administrator*

The hospital's Security Administrator shall be designated by completing a Hospital Security Authorization Form (available from Corporate IS Department) and routing this form to the appropriate parties for processing. System administration functions shall be performed by administrators as delegated by facility management. These individuals shall:

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 6 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00


- (i) Be designated by completing a Hospital Security Authorization Form (available from Corporate IS Department) and routing this form to the appropriate parties for processing.
 - (ii) Follow Information Security Policies and Procedures and report information security incidents to the Corporate Privacy/Security Office.
 - (iii) Ensure systems comply with Information Security Policies and Procedures.
 - (iv) Assess, document, and obtain approvals for exceptions to the Information Security Policies and Procedures.
 - (v) Document procedures specific to security administration at respective entities.
 - (vi) Support the Corporate Privacy/Security Office as requested.
 - (vii) Cooperate with the Privacy/Security Office and Disaster Recovery teams in times of crisis, investigation, planning and testing.
 - (viii) Define user privileges.
 - (ix) Monitor access control logs.
 - (x) Handle system specific access and password issues.
 - (xi) Ensure all appropriate controls are used in the storage, backup, handling, distribution and use of the information assets.
 - (xii) Appoint a backup individual to serve in the place of the Administrator in case the Administrator is unavailable.
- c) *Other Responsibilities*
- Responsibilities of individuals other than those listed above are outlined as appropriate within individual sections of the Information Security Policies and Procedures.

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 7 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

B. Subordinate Policies

Subordinate documents are organized into groups, which taken together, define the Tenet Information Security Policies and Procedures and enable an effective program of information security. These groups of policies cover:

- Record Processing -** Includes definitions of levels of information sensitivity and guidelines for appropriate handling of information including dissemination and disclosure procedures.
- User Security -** Covers important aspects of information security related to management of personnel including access control, user conduct and training.
- Incident Handling -** Defines information security incidents, describes the steps involved in reporting and responding to an incident, and addresses corrective actions that can result from violations of security policies and procedures.
- Physical Safeguards for Information Assets -** Contains standards and procedures supporting the physical security of information and information assets. Topics include development of a facility security plan, control and modification of physical access, and standards for assuring the security of information at workstations.
- Contingency Planning -** Includes requirements for contingency planning and guidelines for the components of the facility's data backup plan, business continuity plan (emergency mode of operations plan), and disaster recovery plan.
- Information Security Administration -** Contains standards and guidelines for the certification of networks and systems, security designs and mechanisms, the use of auditing to assure continuing monitoring of access to systems and applications, and the application of risk management processes to information security.
- Technical Security Administration -** Includes management of the technical aspects of security administration. Topics include management of networks, applications and systems, standards for the use of encryption, data backup, configuration management,

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 8 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

access control, and audit controls.

Biomedical Information Asset Control Defines Biomedical Information Assets and sets forth security controls as they relate to such assets. Topics include: information access controls; information storage, retrieval, and transmission; logging and auditing; security while in use; and business associate agreements.

The complete list of documentation comprising the Tenet Information Security Policies and Procedures is contained in Addendum A.


1. Precedence of the Tenet Information Security Policies and Procedures

The Corporate Information Security Policies and Procedures take precedence over other Information Security policies in Tenet facilities where Corporate Information Security Policies and Procedures are more restrictive.

- a) The Tenet Information Security Policies and Procedures supplement other documentation including corporate level policies, standards and procedures, and Federal, State and Local legislation, codes, rules and regulations. Examples of these are included in Addendum B attached hereto.
- b) Facilities may document their own, more restrictive procedures. The individuals documenting this type of information shall be familiar with the Information Security Policies and Procedures and develop documentation to expand upon the topics.
- c) The duplication of the text of these policies in other policies is discouraged.
- d) A reference to the Information Security Policies and Procedures shall be included in documentation related to these topics.
- e) Where system or application capacities dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in the entity's Information Security Controls Exception Book.

2. Maintenance

Tenet's Privacy/Security Officer is responsible for maintaining this document.

	Information Security Policies and Procedures	No. COMP-Sec 1.0.0
	Title: CORPORATE INFORMATION SECURITY POLICY	Page: 9 of 20
		Revised Date: 12/22/04
		Original Date: 11/06/00

This document contains references to laws, regulations, policies and standards that may change without change to this document. Except as otherwise determined by the Corporate Privacy/Security Office, a change to those laws, regulations, policies and standards does not negate the content or intent of this document.

3. Documentation and Retention Periods

The Privacy/Security Office must maintain the Information Security Policies and Procedures and any action, activity, or assessment required to be documented by these policies or the HIPAA Security Regulations in written (which may be electronic) form. Such documentation must be retained for six years from the date of its creation or the date when it was last in effect, whichever is later. The documentation must be made available to those persons responsible for implementing the procedures to which the documentation pertains. The documentation must be reviewed periodically and updated as needed, in response to environmental or operational changes affecting the security of Tenet’s Information Assets.

C. Definitions

Definitions are maintained in the Information Security Glossary contained in Addendum C.

ADDENDUM A
Tenet Information Security Policies and Procedures

- 1.0.0 Corporate Information Security Policy
- 2.0.0 Record Processing Policy
- 2.1.0 Information Classification Standard
- 2.1.1 Information Handling Procedure
- 3.0.0 User Security Policy
- 3.1.0 Information Access Control Standard
- 3.1.1 Access Request and Modification Procedure
- 3.1.2 Access Termination Procedure
- 3.1.3 Technical, Maintenance and Housekeeping Personnel Supervision Procedure
- 3.2.0 Information Security Awareness Training Standard
- 3.3.0 User Conduct Standard
- 3.3.1 Malicious Software Protection Procedure
- 3.3.2 Password Use Procedure
- 4.0.0 Incident Handling Policy
- 4.1.0 Sanctions Standard
- 4.1.1 Incident Response Procedure
- 4.1.2 Incident Response Procedure for Personal Data about California Residents
- 5.0.0 Physical Safeguards for Information Assets Policy
- 5.1.0 Information Asset Secured Area Protection Standard
- 5.2.0 Information Asset Open Area Protection Standard
- 6.0.0 Contingency Planning Policy
- 6.1.0 Contingency Planning Standard
- 6.1.1 Contingency Planning Procedure
- 7.0.0 Security Administration Policy
- 7.1.0 Security Risk Management Standard
- 8.0.0 Technical Security Management Policy
- 8.1.0 Asset Access Controls Standard
- 8.1.1 UserID Control Procedure
- 8.1.2 Password Control Procedure
- 8.1.3 Encryption Control Procedure
- 8.2.0 Information Asset Administration Standard
- 8.2.1 Change Control Procedure
- 8.2.2 Logging and Auditing Procedure
- 8.2.3 Backup Procedure
- 8.2.4 Malicious Software Control Procedure
- 8.3.0 Network Security Administration Standard
- 8.3.1 Network Administration Procedure
- 8.3.2 Network Access Controls Administration Procedure
- 8.3.3 Network Connections Procedure
- 8.3.4 Network Connection Safeguards Procedure
- 8.3.5 PBX and Voice Mail Procedure
- 8.3.6 Transmission Security Procedure
- 8.4.0 Operating System Security Standard
- 8.5.0 Application Security Administration Standard
- 9.0.0 Biomedical Information Asset Control Policy

ADDENDUM B
Related Documents and References

- Tenet Privacy Policies and Procedures (All)
- Tenet Administrative Policies and Procedures No. 1.9 “Public Release of Information”.
- Tenet Administrative Policies and Procedures No. 1.11 “Records Management”.
- Tenet Administrative Policies and Procedures No. 2.1 “Capital Expenditure Review Process”.
- Tenet Administrative Policies and Procedures No. 2.18 “Coordination of Information Processing Systems”.
- Tenet Administrative Policies and Procedures No. 2.19 “Duplication of Personal Computer Software”.
- Tenet Administrative Policies and Procedures No. 2.25 “Facility Security”.
- Tenet Administrative Policies and Procedures No. 2.35 “Information Systems: Sensitivity, Confidentiality, and Appropriate Use”.
- Tenet Administrative Policies and Procedures No. 2.42 “Reporting of Theft of Assets and Property”.
- Tenet Administrative Policies and Procedures No. 3.3 “Facility Risk Management Reporting Requirements”.
- Tenet Human Resources Policies and Procedures No. 032-f “Access to Personnel Records”.
- Tenet Human Resources Policies and Procedures No. 108 “Confidentiality of Company Information”.
- Tenet Human Resources Policies and Procedures No. 216 “Pre-employment Background Screening.
- 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. 307-F “Employee Orientation”.
- Tenet Human Resources Policies and Procedures No. 401 “Employee Conduct and Work Rules”.
- Tenet Human Resources Policies and Procedures No. 408 “Performance Management”.
- Tenet Human Resources Policies and Procedures No. 513 “Workplace Monitoring”.
- Tenet Human Resources Policies and Procedures No. 804 “Security Inspections”
- Tenet Human Resources Policies and Procedures No. 901 “Termination Of Employment”.
- Tenet Human Resources Policies and Procedures No. 903 “Reductions In Force and Severance Pay”.
- Tenet Human Resources Policies and Procedures No. 904 “Exit Interviews”.

ADDENDUM C

Glossary of Information Security Terms

The following definitions are provided to assist readers of Tenet Healthcare Corporation (Tenet) Information Security Policies and Procedures in understanding the meaning of terms used in individual policies or procedures. Unless otherwise provided in a particular policy, the terms shall have the meanings ascribed to them in this Glossary. Terms not otherwise defined herein, shall have the meaning ascribed to them in the HIPAA Regulations, at 45 C.F.R. Parts 160 and 164.

ADMINISTRATOR OR SYSTEM ADMINISTRATOR OR SECURITY ADMINISTRATOR

The individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases. Duties may include, but are not limited to, installing and configuring system software, performing back-ups and recovery, and adding/removing system users.

APPLICATION LEVEL FIREWALLS

Application firewalls are hosts running proxy servers. The proxy applications are software components running on the firewall.

- Permits no traffic directly between networks.
- Performs elaborate logging and auditing of traffic passing through.
- Performs logging and access control.
- Can be used as network address translators, can mask the origin of the initiating connection.
- Can have a negative impact on performance and may make the firewall less transparent (impact outgoing traffic).

ASSET

Any item that is purchased by, owned by, leased to, contracted by, operated by, used by, controlled by, given to, supplied by, or in any other manner connected to Tenet. This includes everything from pens and paper to mainframe computing systems and other information assets.

AUDIT TRAILS

System, network and application logs, maintenance documents, and any other documentation that would help establish a trail of responsibility in an investigation.

BACKGROUND CHECK

A background check is a complete check of an individual's criminal, civil, and financial status. This includes but is not limited to: local and federal criminal conviction records, lawsuit records, credit bureau records, driver's license records, and military records.

BASTION HOST

A host sitting behind a firewall (router) which is a highly secured and heavily defended. This host is very resistant to attack.

BUSINESS ASSOCIATE

A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, Tenet.

CERTIFICATE AUTHORITY

An entity responsible for the creation, distribution, tracking and revoking of cryptographic keys or digital certificates.

CHANGE CONTROL

Configuration management. The function of tracking changes to assets. This encompasses, without limitation, changes to hardware, software, and networks.

CLASSIFIED

Any information, regardless of its format or media, that is “NON-PUBLIC” or has been assigned a security classification such as PROPRIETARY or CONFIDENTIAL.

CLIENTS / CUSTOMERS

Any individual, groups of individuals, companies, organizations, etc. which do business with Tenet.

CONFIDENTIAL

Information that is protected above the PROPRIETARY level. See the Information Classification Standard 2.1.0 for further information.

CONFIDENTIALITY

Confidentiality is the degree to which the privacy or secrecy of something can be trusted.

CONFIGURATION MANAGEMENT

See Change Control.

COPYRIGHT

“A body of legal rights that protect creative works from being reproduced, performed, or disseminated by others without permission. The owner of copyright has the exclusive right to reproduce a protected work; to prepare derivative works that only slightly change the protected work; to sell or lend copies of the protected work to the public; to perform protected works in public for profit; and to display copyrighted works publicly. These basic exclusive rights of copyright owners are subject to exceptions depending on the type of work and the type of use made by others.”

“The term work used in copyright law refers to any original creation of authorship produced in a tangible medium. Thus, works that can be copyrighted include literary pieces, musical compositions, dramatic selections, dances, photographs, drawings, paintings, sculpture, diagrams, advertisements, maps, motion pictures, radio and television programs, sound recordings, and-by special legislation passed by the Congress of the United States in 1980-computer software programs.”

“Copyright does not protect the idea or concept; it only protects the way in which an author has expressed an idea or concept. If, for example, a scientist publishes an article explaining a new process for making a medicine, the copyright prevents others from substantially copying the article, but it does not prevent anyone from using the process described to prepare the medicine. In order to protect the process, the scientist must obtain a patent.”

From Microsoft Encarta 96 Encyclopedia

DATA

Data is, without limitation information of any kind that is collected, stored, transmitted, and/or printed. (i.e. A software program such as a spreadsheet, with no information added, has no data. When information is added, it contains data).

Tenet Healthcare Corporation

DATA CENTER

A central location containing computer assets including, but not limited to, servers, magnetic storage devices, and network devices. This data center could service a single building or department, or serve a large geographical area.

DIGITAL CERTIFICATE

A cryptographic signature used to provide irrefutable evidence of origin.

DUAL-HOMED GATEWAY

A dual homed gateway runs proxy software and has two network interfaces. One interface for each network (outside, inside). All traffic passing through is blocked.

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)

Protected Health Information that is created, received, maintained, or transmitted in electronic form by or on behalf of a covered entity.

ENCRYPTION

The transformation of plaintext (words) into cipher text (unintelligible) by cryptographic techniques to protect data from disclosure during network transmissions.

EXTRANET

A network connection between two companies. This does not have to be a geographical separation. If a company data center houses not only their own systems, but also those of a client, and a 10-foot cable separates the two systems, that cable constitutes an external connection.

FACILITY

A hospital, clinic, laboratory, office, site or building that is owned, leased, used or affiliated with Tenet.

FACILITY MANAGEMENT

The individuals responsible for the management at a Facility, including, but not limited to, the CEO, CFO, CIO, CNO, COO or their designated appointees.

FILE, DATA or OBJECT ADMINISTRATOR

An individual delegated the authority and responsibility with respect to a file, set of files, or discreet data, too:

- Determine classification.
- Determine access authority.
- Assign custody.
- Specify physical controls over input and output.
- Determine the need for alternative processing capabilities.
- Monitor compliance with control requirements.

FIREWALL

A device or series of devices that separate and secure a company's internal networks from external networks, or, in some cases, sensitive internal networks from general internal networks.

GUIDELINES

Procedures that show a ‘best practices’ approach to an issue, but do not mandate compliance. Reasons for non-compliance and alternative solutions shall be documented.

HARDWARE

The physical part of a computer system including the machinery and equipment.

HEALTH PROFESSIONAL

An individual who:

- has undergone formal training in a health care field;
- holds an associate or higher degree in a health care field, and holds a state license or state certificate in a health care field; and
- has professional experience in providing direct patient care.

HOST (or router) BASED AUTHENTICATION

This authentication takes place when the firewall is a router and is using IP addresses to allow or disallow access. This configuration is vulnerable to "IP Spoofing" attacks.

HYBRID OR COMPLEX GATEWAY

This is the combination of different types of firewalls. If those firewalls are set up in parallel, they do not complement each other (they do not increase the security of the network). The vulnerabilities on one firewall could allow an intruder to bypass the other firewalls. If they are set up in series, the features of each are combined to present a more complete protection package.

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Information that is a subset of health information, including demographic information collected from an individual, and that:

- Is created by or received from a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and
- Which identifies the individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

INFORMATION ASSET OR RESOURCE OR ASSET

Without limitation, any computer, network, electronic file, record, service, hardware, software, regardless of type or media, that is purchased by, owned by, leased to, contracted by, operated by, used by or controlled by Tenet. This is to include ALL data residing in, or generated by those resources regardless of its format or storage device.

INFORMATION SECURITY

The protection of data against loss, modification, or unauthorized disclosure during its input to, storage in, or processing by a computing resource or at any point thereafter. The protection of computing resources from physical or logical damage, or any other act or occurrence that could decrease or degrade system availability.

INTEGRITY

Integrity is the degree to which something is free from corruption, i.e. protected from being damaged, altered, added or removed.

INTELLECTUAL PROPERTY

Intellectual Property is defined as ownership, copyrights, licenses, trademarks, data, programs, inventions, ideas, information, documentation, programs, inventions, formulas, procedures, and any other material, real or imagined, generated by an individual while working at or for Tenet Healthcare Corporation.

INTERNET

A worldwide "network of networks" that uses Transmission Control Protocol/Internet Protocol (TCP/IP) for communications.

INTRANET

A web based, browser accessed, internal service which allows Internet like searches and access for a company's internal use.

IP

Internet Protocol.

LAN (Local Area Network)

An interconnected system of computers and peripherals. LAN users can share data stored on hard disks in the network and can share printers connected to the network. Access to a LAN is normally restricted to internal users; access from outside the LAN is normally controlled by a firewall.

LOGGING

The act of writing information to a log file.

LOGS

A file on a system that records events. This can include:

- System logs with startup, shutdown, errors and other information.
- Database logs showing access, changes.
- Application logs
- Network logs

MALICIOUS SOFTWARE

Unauthorized programs or code that have been introduced into organizational software with the intent to, and purpose of, causing damage to data, applications, or networks. Malicious code includes viruses, time bombs, logic bombs, Trojan horses, and worms.

MODEM

Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system.

NEED TO KNOW

The "Need To Know" concept indicates that permission to access or view something is not authorized in a general manner. Each individual being authorized access to data shall have a proven "need to know" which can be determined by their job description, authorized duties, real duties or by management decision. With limited exceptions, individuals must limit uses and disclosures of, and requests for, Protected Health Information (as defined below) to the minimum necessary to

accomplish the intended and permitted purpose of the use, disclosure or request of this information. Tenet's Privacy Policies and Procedures define the minimum necessary information required by workforce members with specific job responsibilities and procedures for handling exception situations. Individuals must adhere to these policies and procedures.

NETWORK LEVEL FIREWALL

Also called a "screened host firewall". Controls the access to a single host. Uses a router operating at the network level. The host is a bastion host. Decisions are based on the source, IP addresses and ports in individual IP packets. These firewalls can range from "simple" (a router), to much more sophisticated firewalls that maintain internal information about, but not limited to, the connections passing through them and the contents of data streams. This level of firewall can route traffic directly through the firewall. An incoming transmission must (usually) have a valid IP address.

OPT-IN

Agreement by a user to participate in an activity or function of the Web site, provided after the Web site has fully disclosed the terms and conditions of participation to the user.

OPT-OUT

A process by which a user declines to participate in an activity or function of the Web site.

OWNER OF INFORMATION ASSET OR INFORMATION ASSET OWNER

The individual or group of individuals who own an information asset, and have authority to decide whether or not that system is necessary. This role typically resides with the Director of the department that has primary responsibility for the system's use.

PASSWORD

A secret code that is selected by each registered computer user and which, when recognized by a system's security program, in conjunction with the UserID, allows the user to access the computer system.

PASSWORD BASED AUTHENTICATION

Authentication based on a unique UserID and password combination to determine access.

PATENT

"Patent, in law, the abbreviated term for letters patent, in its most general sense a document issued by a government conferring some special right or privilege. In the U.S. the term is now restricted principally to patents for inventions granted under federal statute. The specific attributes of novelty of the item for which a patent is sought are called claims. A patent gives the inventor the exclusive privilege of using a certain process or of making, using, and selling a specific product or device for a specified period of time."

From Microsoft's Encarta 96 Encyclopedia

PBX

Private Branch Exchange, a telephone switching system used internally to route calls from external lines to internal extensions. Controls, in part, voice mail and call forwarding.

PC

See Personal Computer.

PERSONAL COMPUTER

A computing device which contains its own memory, processing, storage and I/O devices, and which is intended for use by a single individual or a very small number of individuals.

PHI

See Protected Health Information.

PHYSICAL SECURITY

The protection of personnel, information assets, facilities, and utilities against intrusion, disclosure, theft, damage, destruction or misuse.

PUBLIC KEY INFRASTRUCTURE (PKI)

A public-key cryptography method that is implemented through the use of security architectures, techniques, practices, and procedures.

PROPRIETARY

All non-PUBLIC and non-CONFIDENTIAL Tenet information. See the Information Classification Standard 2.1.0 for further information.

PROTECTED HEALTH INFORMATION (PHI)

Individually Identifiable Health Information (IIHI) that is transmitted by electronic media; maintained in any medium as described in the definition of electronic media; or transmitted or maintained in any other form. PHI excludes IIHI in education records and student health records covered by the Family Educational Rights and Privacy Act (FERPA), and employment records held by a Covered Entity in its role as employer.

PROXY SERVER

See APPLICATION FIREWALL. Proxies can be modified to allow or disallow specific services, (i.e. an FTP proxy can be configured to permit incoming FTP while block outgoing FTP).

REMOTE ACCESS

Access to Tenet information resources from outside the established LAN/WAN environment.

SECURITY OFFICER

The person designated by Tenet to be responsible for the development and implementation of the privacy policies and procedures of Tenet.

SECURITY VIOLATION

A failure in the physical security and/or Information Security measures resulting in a loss of data, the inability to provide computing services, unauthorized use or modification of information assets, or the unauthorized access to files, data, and services.

SOCIAL ENGINEERING

The process used by persons intent on gaining illegal access to Tenet's computing assets (disgruntled associates, intruders, industrial spies, etc.) to gather information by impersonation, fraud, lying, intimidation and social interaction.

SOFTWARE

The computer program that instructs computer hardware to perform an action. System software is the operating system that controls the basic functioning capabilities of the computer, network software

enables multiple computers to communicate with one another, and language software is used to develop programs.

TCP

Transmission Control Protocol.

TERMINAL

A terminal is the end point in a computing environment where an individual interfaces with a computer, network or other information asset. The following are examples of a terminal:

- A personal computer in stand-alone mode.
- A personal computer when connected to a network.
- A “dumb” terminal (normally just a CRT and a keyboard).
- A bio-medical device, which takes input from an individual.
- A handheld computing device (PalmPilot, barcode scanner).

THREAT

Any circumstance or event with the potential to cause harm to an information asset.

TRADEMARK OR SERVICE MARK

“A Trademark is any symbol, such as a word, number, picture, or design, used by manufacturers or merchants to identify their own goods and distinguish them from goods made or sold by others. Thus, a trademark identifies the source of a product and fixes responsibility for its quality. If customers like the goods, the trademark enables them to know what to purchase in the future; if they dislike the product, they will avoid goods with that trademark.”

“The name of a type of product cannot be a trademark, because every maker of that product is free to use its name. Sony, for example, is a well-known trademark for televisions, radios, and audio equipment, but no one can have trademark rights to the word television or radio. On several occasions, however, words intended by manufacturers to be used as trademarks for new products were instead used by customers to name the products; such words then lost their legal status as trademarks. Examples include aspirin, cellophane, and escalator.”

From Microsoft's Encarta 96 Encyclopedia

For most intents and purposes, a SERVICE MARK is the same as a TRADEMARK.

TRUSTED NETWORK

Networks within a company's LAN/WAN environment perimeter defense which comply with the company's security policies.

UNTRUSTED NETWORK

Networks, normally outside a company's LAN/WAN environment and perimeter defenses, which are not subject to a company's security policies.

UPS

Un-interruptible power supply. A device that isolates the power provided to an asset from the commercial supply. This is done by taking in the commercial supply, converting it to DC, charging a set of batteries, converting the battery output to AC, and providing that to the asset.

USER

Users that input/output data to/from Tenet information assets. These individuals are collectively referred to as Users, and may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, business partners and electronic (web site) visitors.

USERID

A unique identification code used by an information asset to identify an individual gaining access to that asset. When the UserID is matched with the appropriate password, access is granted and the process uses the UserID to set access privileges for resource allocation, batch or interactive processes, file or record ownership.

VIRUS

A computer virus is an unauthorized program that replicates and spreads through computing assets onto various data storage media (floppy disks, magnetic tapes, hard drives, etc.) and/or across a network, or resides in memory.

VPN (VIRTUAL PRIVATE NETWORK)

A VPN is a secured external network that uses encryption to secure a link between two sites across a public network. All traffic across the network is encrypted by the VPN, not by the individual users. This allows the sites to verify the data is from the specified source, that the data has not been modified, and ensures that a person who intercepts a data block between the two sites cannot read the data. A VPN is not restricted to a public network, but can be used with leased lines as well.

VULNERABILITY

A bug or feature in an information asset that enables an attacker to circumvent security measures.

WEB SITE

A source of health content, commerce, connectivity, and/or care delivery that users access via the Internet or other electronic means.

WORKFORCE

Workforce includes employees, volunteers, trainees and other persons, whose conduct, in the performance of work for the facility, is under the direct control of such facility, whether or not they are paid by the facility. Workforce excludes independent contractors of the facility because the facility may not exercise direct control over an independent contractor. Workforce also excludes Business Associates or an employee, agent or contractor of a Business Associate.

WORKSTATION

See Terminal.

ZEROIZATION

The act of electronically writing a series of zeros (0s) over a magnetic media to ensure that the data formerly stored on that media is no longer readable or recoverable.