	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 1 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

I. PURPOSE:

The purpose of the standard is to provide standards that 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. 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.


II. DEFINITIONS:

- A. “**Administrators**” mean the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.
- B. “**Cloud Storage**” refers to the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or personal computer.
- C. “**Confidential Information**” shall have the same meaning as Proprietary Information.
- D. “**Proprietary Information**” means any trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, customer, patient, employee, investor, or business information, whether in oral, written, graphic or electronic form.
- E. “**Users**” mean individuals 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.
- F. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.

III. STANDARD:

- A. 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 process of routine and non-routine receipt, creation, manipulation, storage, dissemination, transmission, and/or disposal. It is expected all Users will maintain the confidentiality of this information. Tenet

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	2 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06

information asset Users will be provided access to Proprietary Information based on their need to know and job requirements.

1. Each User of PHI must have an individual UserID and confidential password for accessing that information.
2. Access to PHI will be managed through active administrative, technical, and physical access controls.

a. Routine and Non-Routine Receipt and Creation

All PHI and other Proprietary Information created or received by Users of Tenet information assets is the property of Tenet.

b. Routine and Non-Routine Manipulation

(1) Compliance Officers and Information Security Officers shall assist information owners to define the procedures governing the movement, assembly and maintenance of PHI and other Proprietary Information.


(2) Storage

(a) Tenet does not authorize the storage of sensitive authentication data (SAD) post transaction authorization or any customer cardholder data (CHD) beyond the last four digits of the customer's payment card number, expiry date, and customer name.

(b) PHI must be archived and maintained in a secure manner, whether within the Tenet Facility, at off-site locations, or at Vendor-owned locations.

(c) Proprietary Information and PCI Data stored on computer media (including backup tapes, CDs, flash/zip drives, etc.) must be encrypted using the Data Encryption method outlined in EC.PS.04.05 Technical Controls Security Standard.

(d) Compliance Officers and Information Security Officers must implement standards and procedures for their local environment that meet the requirements of Tenet's standards and

	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 3 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

Administrative policy AD 1.11 Records Management and its Record Retention Schedule.


- (e) Confidential information in hardcopy form or on computer readable media must be stored in secure fashion when not in use. Options for secure storage include, but are not limited to:

- A locked file cabinet
- A safe
- A secured room

(3) Routine and Non-routine Dissemination

Information may be disseminated or transmitted in a variety of formats, including electronic (e-mail, File Transfer Protocol, Electronic Data Interchange), hard copy, or other media, and must always be accomplished in accordance with the policies appropriate to the classification level of the data.

- (a) Proprietary Information must be limited to individuals who have a “need to know.”
- (b) PHI must not be disclosed unless authorized by law, the patient, or when a defined medical emergency exists.
- (c) Compliance Officers and Information Security Officers will assist information owners to define rules of distribution of Proprietary Information and review those rules routinely to validate the application of need to know principles.
- (d) When using storage media (tapes, floppies, CDs, flash/zip drives, etc.) to send information to a third party, an inadvertent disclosure of previously recorded information must be avoided. All computer storage media being sent to a third party must be:
- (i) Unused media, or

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	4 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06

- (ii) Cleansed using a zeroization or degaussing process in accordance with approved procedures (See Administrative policy AD 1.11 Records Management and its Record Retention Schedule for further information), and then reformatted before being used.

(e) Data Requests from Outside Sources

- (i) Direct requests for PHI should be directed to the Tenet Facility Health Information Management Department or Medical Records Department.
- (ii) Refer to Administrative policy AD 1.09 Media Relations and Public Release of Information for information regarding requests for other Proprietary Information.

(f) Transmission

Transmission of information is the transfer of data between applications, systems, companies, or personnel. See ES.PS.04.05 Technical Controls Security Standard for additional information on this topic.


(g) Disposal

- (i) PHI must be destroyed by shredding or incineration.
- (ii) Other Proprietary Information must be disposed according to Administrative policy AD 1.11 Records Management and its Record Retention Schedule.

B. Workstation Use

A workstation is any point of access to Tenet's information assets including, without limitation, computer terminals, personal computers, laptops, and hand held computing devices.

1. In a shared environment, where a computing resource is used by more than one individual (such as a nursing station), Users must exit from any

	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 5 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

applications where their personal UserID and password were used before leaving the workstation.

2. In a non-shared environment (such as an office cube setting), Users must apply a password protected screen saver in accordance with ES.PS.04.05 Technical Controls Security Standard.
3. At the end of each work shift, Users must lock or log off of their workstations so as to restrict access to that workstation to only authorized Users.
4. All workstations, terminals or other monitors must be equipped with automatic logoff or a password required screen saver.
 - a. The automatic log off function must be set to occur after fifteen minutes of inactivity for the workstation environment.
 - b. The password-protected screen saver, if used, must be set to activate after an inactivity period appropriate for the environment. It is strongly recommended that the screen-saver activate no greater than after fifteen minutes of inactivity, but the exact time settings should be determined by the Compliance Officer and Information Security Officer.
 - c. The password function shall be active and conform to EC.PS.04.02 User Security and Conduct Standard.


C. Handling of Proprietary Information

Users of Tenet Proprietary Information must apply the following standards that shall assist in protecting the confidentiality, availability, and integrity of this information.

1. Inadvertent Viewing of Information

Unauthorized individuals may inadvertently view Proprietary Information simply by looking at material on a desk or nurses' station, or by looking at a computer screen. If an individual inadvertently views Protected Health Information (PHI), this disclosure may need to be accounted for as outlined under EC.PS.03.05 Accounting of Disclosures Standard. The following safeguards must be implemented to prevent these disclosures:

- a. Screens on information assets that display Proprietary Information must not be legibly visible from outside the immediate work area. They must be positioned to restrict viewing from hallways,

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	6 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06


reception areas, waiting rooms, and other public areas, and/or a filter restricting the angle for viewing a screen may be employed.

- b. If an unauthorized person enters an area where Proprietary Information is present, steps to conceal the information must immediately be taken.
 - (1) Information on paper documents can be covered with other material or one-sided documents can be turned over to face down.
 - (2) Information displayed on a computer screen must be protected by a password-protected screen saver or the User shall log-off. It is recommended that this password-protected screen saver activate no greater than after fifteen (15) minutes of inactivity, but the exact time settings should be determined by Tenet Facility management.
- c. At the end of the work shift, users must take reasonable efforts to secure Proprietary Information, including locking office doors, drawers and filing cabinets whenever possible.

2. Copying and Printing Information

Making additional copies or printing extra copies of Proprietary Information should only be conducted when necessary.

- a. Users must not leave the machine unattended during the copying process. The machine should be attended until the originals and all copies of the Proprietary Information are removed from the machine.
- b. Proprietary output must be delivered directly to the designated recipients. Such output must never be delivered to unsecured locations, such as unattended desks or unoccupied offices.
- c. If a copy machine, printer, or other reproduction machine jams or malfunctions, Users must not leave the machine until all copies of Proprietary Information are removed.
- d. Waste copies of /Proprietary Information generated in the course of copying, printing, or otherwise handling such information must be destroyed according to Administrative policy AD 1.11 Records Management and its Record Retention Schedule.

	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 7 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

3. Electronic Communications

a. Instant and Text Messaging

Use of any form of unsecured Text or Instant Messaging (*e.g.*, ICQ, AOL Instant Messenger, MSN Messenger, Yahoo Messenger) to transmit Proprietary Information is prohibited unless it meets the requirements of EC.PS.04.10 Text Messaging Standard.

b. Personal Mobile Data Devices

Use of unauthorized personal smartphones, tablets, and similar devices (collectively “mobile data devices”) to create, store, access, transmit or receive ePHI or other Proprietary Information is prohibited unless secured in accordance with the Tenet approved Bring Your Own Device (BYOD) and Mobile Data Management (MDM) system standard.


c. Information By Email

Tenet approved email systems must be used to transmit Proprietary Information.

- (1) Email containing PHI or other sensitive Proprietary Information sent outside of the Tenet trusted network must be sent encrypted. To ensure your email is encrypted, follow the directions on the “Encrypt Email” link located at the eTenet Information Security Help Center page.
- (2) A confidentiality statement must be included with all email transmissions sent outside of the Tenet trusted network (see Attachment A, Sample Confidentiality Statements).
- (3) Use of unauthorized email systems (*e.g.*, Hotmail, AOL Mail, Yahoo Mail, Gmail), to transmit Proprietary Information is prohibited.

d. Information by Fax

Faxing Proprietary Information should only be conducted if the following rules are observed (see Fax Facts on eTenet for additional information):

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	8 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06

- (1) If the Fax number has not been previously used, a cover sheet shall first be sent and acknowledged by the recipient. After this test is performed, the Proprietary Information may be sent.
- (2) Unless no other transmission alternative is available and information must be transmitted, Proprietary Information must not be faxed via intermediaries (*e.g.*, hotel staff, rented mailbox store staff).
- (3) A cover sheet must be sent as the lead page of the fax. This cover sheet shall include the following information:
 - From: Originator's name, company and telephone contact number.
 - To: The recipient's name, company fax number and telephone number.
 - A confidentiality statement.
 - The number of pages in the fax, including the cover sheet.

4. Internal Dissemination of Proprietary Information


Proprietary Information may be disseminated internally as follows:

- a. By hand delivery directly to the addressee or a secure area (not left on desks or in unprotected mail slots); or
- b. By internal mail, if it is securely enclosed in an envelope and marked with the appropriate address and as "Confidential" only.

5. Information on the Phone

Proprietary Information may be communicated over telephones using the following guidelines:

- a. Proprietary Information must not be discussed on speakerphones unless all participating parties first acknowledge that unauthorized individuals are not in close proximity.

	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 9 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

- b. Users must speak in guarded terms and refrain from mentioning Proprietary details beyond those needed to communicate the information.

6. Public Discussions

Users must refrain from discussing Proprietary Information when holding discussions in public (*e.g.*, hallways, elevators, cafeterias, restrooms). Reasonable safeguards (*e.g.*, lowering voices, changing location) should be taken to limit inadvertent disclosures of PHI and other Proprietary Information.

7. Information in Meetings


When Proprietary Information is released in a meeting, the speaker must clearly communicate the sensitivity of the information.

- a. The speaker must remind the audience to use discretion when disclosing it to others.
 - b. Visual aids such as slides and overhead transparencies shall include a “Confidential” label.
 - c. Attendance at meetings where Proprietary Information is discussed must be adequately controlled.

8. Taking Information Off-Site

Proprietary Tenet information (which includes, without limitation, portable computers with solid-state disks (SSD), hard disks, floppy disks, hard-copy output, and paper memos) must not be removed from Tenet unless such removal is part of the User’s required job responsibilities. When taking Tenet information off-site, Users must ensure that:

- a. Proprietary Information is not left unattended unless it is maintained in a secure location.
 - b. Appropriate safeguards are implemented when transporting PHI and other Proprietary Information, including paper copies of PHI, portable computers storing PHI, and electronic media storing PHI. Vehicles containing Proprietary Information must be kept locked while unoccupied, and Proprietary Information must be stored in a secured location (*e.g.*, locked glove box, trunk) when possible.

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	10 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06

- c. Proprietary Information must not be read, discussed, or otherwise exposed in public places, such as airplanes, public transportation, or restaurants.

9. Cloud Storage

Tenet Confidential or Proprietary Information shall not be stored in unapproved cloud storage (e.g., Dropbox, Google Drive, Microsoft OneDrive) by any User.

IV. PROCEDURE:

A. Implementation


1. Information Privacy and Security Program

a. Tenet Facility WITHOUT Regional Privacy Officer

- (1) The Tenet Facility Compliance Officer and Tenet Facility Information Security Officer, the Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of the Information Privacy and Security Program (the “Program”) Standards at the facility level.
- (2) Tenet Facility Leadership will:
 - (a) Adopt this standard and where necessary develop specific written procedures in order for the Tenet Facility to operationalize this standard;
 - (b) Develop appropriate methods to monitor adherence to the written procedures; and
 - (c) Report monitoring activity to the Tenet Facility Compliance Officer.

b. Tenet Facility WITH Regional Privacy Officer

- (1) The Regional Privacy Officer, Tenet Facility Information Security Officer, Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of Program Standards at the facility level.

	Information Privacy and Security Program	No.	EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page:	11 of 12
		Effective Date:	07-13-17
		Retires Policy Dated:	10-27-16
		Previous Versions Dated:	09-16-13; 01-11-06

(2) Tenet Facility Leadership, in coordination with the Regional Privacy Officer and Tenet Facility Compliance Committee, will create specific policies and procedures as necessary in order for the Tenet Facility to operationalize the Program.

(3) Tenet Facility Leadership will report Program monitoring activity to the Regional Privacy Officer.


c. Corporate Office (Dallas/Nashville)/Region/Market

(1) Tenet's Information Privacy/Security Office will work with the Regional Privacy Officers, Tenet Facility Compliance Officers, Tenet Facility PIRTS, Tenet Facility Information Security Officers, Tenet Facility Compliance Committees, and Tenet Facility Leadership to develop, maintain, and update policies, procedures and standards for protecting the privacy of PHI and affording patients their rights with respect to their PHI.

(2) Tenet Corporate Office and Tenet Region/Market Offices must incorporate these standards into their specific policies and procedures where necessary.

V. REFERENCES:

- Administrative policy AD 1.09 Media Relations and Public Release of Information
- Administrative policy AD 1.11 Records Management and its Record Retention Schedule
- EC.PS.03.05 Accounting of Disclosures Standard
- EC.PS.04.00 Information Security Policy
- EC.PS.04.02 User Security and Conduct Standard
- EC.PS.04.05 Technical Controls Security Standard
- Regulatory Compliance policy COMP-RCC 4.21 Internal Reporting Of Potential Compliance Matters
- Information Privacy & Security Glossary of Definitions
- eTenet Information Security Help Center
- eTenet Fax Facts

	Information Privacy and Security Program	No. EC.PS.04.01
	Title: RECORD PROCESSING & INFORMATION HANDLING STANDARD	Page: 12 of 12
		Effective Date: 07-13-17
		Retires Policy Dated: 10-27-16
		Previous Versions Dated: 09-16-13; 01-11-06

VI. ATTACHMENTS:

- Attachment A: Sample Confidentiality Statements for Email
- Attachment B: Sample Fax Cover Sheet

SAMPLE CONFIDENTIALITY STATEMENTS FOR EMAIL

- Sample 1: “The information in this communication is confidential and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication.”
- Sample 2: “The information in this communication is confidential and may be privileged, and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication.”

SAMPLE FAX COVER PAGE

Facility Logo

Street Address
CITY, STATE ZIP
tel: XXX-XXX-XXXX
fax: XXX-XXX-XXXX
www.facilityWebaddress.com

fax cover

Date	Pages (including cover sheet)
To	From
Title	Title
Company	Company
Tel	Tel
Fax	Fax
Please confirm you received this transmission by calling:	

Message/Comments:

Confidentiality Notice: The information in this communication is CONFIDENTIAL and is directed only to the intended recipient. Please do not forward this communication without my permission. If you have received this communication in error, please notify me immediately and delete/destroy this communication.