	Information Privacy and Security Program	No. EC.PS.04.10
	Title: TEXT MESSAGING STANDARD	Page: 1 of 5
		Effective Date: 11-30-18
		Retires Standard Dated:
		Previous Versions Dated:

I. SCOPE:

This standard applies to (1) Tenet Healthcare Corporation and its wholly-owned subsidiaries and affiliates (each, an “Affiliate”); (2) any other entity or organization in which Tenet Healthcare Corporation or an Affiliate owns a direct or indirect equity interest of greater than 50%; and (3) any hospital or healthcare facility in which an Affiliate either manages or controls the day-to-day operations of the facility (each, a “Tenet Facility”) (collectively, “Tenet”).

II. PURPOSE:

This standard is designed to address text messaging and the associated risks of business communications and ensuring that any messaging is consistent with Tenet’s Information Privacy and Security Program policies, Tenet’s Standards of Conduct, applicable state privacy laws and federal privacy laws.


III. DEFINITIONS:

Terms used herein are defined in EC.PS.01.00 Information Privacy and Security Administration Policy, Attachment A – Glossary of Definitions.


IV. STANDARD:

Effective security of confidential, proprietary and/or protected health information communicated electronically is the responsibility of every facility workforce member and affiliate, who has access to the facility’s confidential, proprietary and/or protected health information. It is the responsibility of every user to know this standard and to conduct their activities accordingly.

- A. Except as provided in this policy, text messaging which contains confidential, proprietary or protected health information shall be carried out only through secured messaging applications approved by Tenet.
- B. All users must receive approval to use secured texting for any business purpose involving confidential or proprietary information.
- C. Upon implementation of secured texting application, the Tenet Facility is responsible for preparing a written policy and procedure consistent with this standard and identifying the authorized user groups for the facility. *See Attachment A for a model policy meeting the requirements of this element.*
- D. The Tenet Facility Information Services Director (ISD), or their designee, shall:
 1. Maintain a list of all approved active users and the mobile devices used for texting EPHI (whether facility-owned or personal devices). The list will include at a minimum:

	Information Privacy and Security Program	No. EC.PS.04.10
	Title: TEXT MESSAGING STANDARD	Page: 2 of 5
		Effective Date: 11-30-18
		Retires Standard Dated:
		Previous Versions Dated:

- a. Name of approved user;
 - b. Title
 - c. Mobile device number, facility or personally owned;
 - d. Department and;
 - e. Approving Supervisor or Approving Sponsor.
 2. Deactivate the credentials issued to the user on their last day of employment or affiliation with the Tenet Facility.
- E. All Workforce members permitted to utilize secured texting under these guidelines must do so in compliance with this standard, Tenet policies and the Tenet Facility's written policy.
1. Employees who utilize their personal devices for business related texting must do so voluntarily and at their expense as using their personal devices is not a condition of employment.
 - a. Employees shall be notified that communications made with their personal device for Tenet business purposes are not private or confidential and may be viewed by Tenet at any time. Compliance with this standard is a condition of employment.
 - b. Any communication which is private, confidential or personal shall not be placed on Tenet's information systems. Any text message that is created, sent or received and that any file in the computer network, in local PCS or on disks located on Tenet property may be read or listened to at any time. Tenet expressly reserves the right to intercept, read, review, access and disclose all text messages, including, but not limited to Internet usage and Web sites that you have accessed. Use or log on to these devices constitutes consent to these to such actions. The reasons include without limitation, to investigate wrongdoing, to determine whether security breaches have occurred, to monitor compliance with policies and to obtain work product needed by other employees. Tenet will respect the privacy of employees' and will only request access to the personal device in order to respond to compliance audits, monitoring or investigations and/or discovery requests arising out of administrative, civil, or criminal proceedings.
 - c. Tenet reserves the right to monitor, prohibit, restrict, block, suspend, terminate, delete or discontinue access to any work-related text messaging solution without notice and at its sole discretion. Any work-

	Information Privacy and Security Program	No. EC.PS.04.10
	Title: TEXT MESSAGING STANDARD	Page: 3 of 5
		Effective Date: 11-30-18
		Retires Standard Dated:
		Previous Versions Dated:


related text messaging that does not adhere to Tenet's policies must be terminated.

- d. All workforce members granted credentials to utilize the Tenet approved secured messaging solution must have the Tenet approved mobile device management application installed and configured to the Tenet standard prior to use of the secured messaging solution.

2. Authorization for secured texting is for on-duty time only.

F. Permitted uses and disclosures related to secured texting:

1. Protected Health Information (PHI) that is to be transmitted electronically shall be transmitted in a manner that is protected against unauthorized access and ensures its integrity. In order to accommodate both the need of protecting the PHI and the need for efficient communication of PHI in support of patient care, PHI may be transmitted electronically only when the use or disclosure is permitted and in accordance with other existing policies, and also when the circumstances described herein are met. When electronic transmission of PHI is allowed within these parameters, reasonable and appropriate security measures shall be implemented.
2. If PHI is contained in the secured text message, the staff member or provider will document in the medical record any PHI that is sent or received via text and is used to make a treatment decision about a patient.
3. Under no circumstances may secured text messages be used:
 - a. As a substitute for computerized physician order entry (CPOE), to place or clarify physician orders.
 - b. To communicate critical values.
 - c. To communicate photos for diagnostic or interpretive purposes.
 - d. To communicate with a patient, their representative, family members or friends.
4. Employees who voluntarily use their personal devices while on duty under this guideline:
 - a. Upon termination of employment, the employee will
 - (1) Attest that they do not retain any Tenet or Tenet facility information or applications on their personally owned devices or on any backed up copies of their device.


	Information Privacy and Security Program	No. EC.PS.04.10
	Title: TEXT MESSAGING STANDARD	Page: 4 of 5
		Effective Date: 11-30-18
		Retires Standard Dated:
		Previous Versions Dated:

- b. Upon termination of employment, the ISD or their designee,
 - (1) Shall deactivate the user's credentials to the secured messaging solution on their final day of employment.
 - c. Employees with access to patient health information shall notify their approving supervisor or sponsor and the ISD, or their designee:
 - (1) before selling or disposing of their portable mobile device, and
 - (2) Immediately report when the device is lost or stolen.
 5. In **limited** circumstances, unsecured texting of **limited** EPHI to ensure the immediate care and safety of the patient will be permitted. Examples include:
 - a. Symptoms and preliminary assessment information.
 - b. Sharing pertinent information with an on-call physician; *e.g.*, images of an EKG strip or wound.
 - c. Using Face Time or Skype for Business.
 - d. If EPHI is contained in the text message, the staff member or provider will document in the medical record any EPHI that is sent or received via text and is used to make a decision about a patient.
 - e. All texts and images that include EPHI must be deleted immediately. If retention is necessary, the retention period for maintaining EPHI on mobile devices shall be no longer than 48 hours.
 6. The Tenet facility shall ensure asset disposal consistent with the Information Security standards related to Tenet owned assets containing protected health information or personally identifiable information.

V. IMPLEMENTATION:

A. Implementation

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

	Information Privacy and Security Program	No. EC.PS.04.10
	Title: TEXT MESSAGING STANDARD	Page: 5 of 5
		Effective Date: 11-30-18
		Retires Standard Dated:
		Previous Versions Dated:

2. Tenet Facility 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 Privacy and Security Compliance Officer.

B. Corporate Office

1. Tenet's Information Privacy and Security Office, through the Privacy and Security Compliance Officers, will work with the Tenet Facility Information Security Officers Tenet Facility PIRTs, and Tenet Facility Compliance Committee to develop, maintain, and update procedures and standards for protecting the privacy of PHI and other Confidential/Proprietary information and affording patients their rights with respect to their PHI.
2. Tenet Corporate Office must incorporate these standards into their specific policies and procedures where necessary.

VI. REFERENCES:

- EC.PS.01.00 Information Privacy and Security Administration Policy
- EC.PS.02.00 Patient Information Privacy Policy
- EC.PS.03.00 Patient Rights Policy
- EC.PS.04.00 Information Security Policy
- HR.ERW.18 Use of Information and Technology Systems

VII. ATTACHMENTS:

- Attachment A: Request for Access to Secured Messaging Application
- Attachment B: Attestation of Removal of Tenet and Tenet facility information
- Attachment C: Model Facility Text Messaging Policy