[Insert Hospital Logo]	Information Privacy and Security Program	No. EC.PS.04.10.01
	Title: **MODEL FACILITY TEXT MESSAGING POLICY**	**Page:** 1 of 5
		Origination Date: 11-30-18
		Effective Date: xx-xx-xx
		Retires Standard Dated: xx-xx-xx
		Previous Versions Dated: xx-xx-xx
		Privacy and Security Compliance Approval Date: xx-xx-xx
		Hospital Governing Board Approval Date: xx-xx-xx

I. SCOPE:

This policy applies to any member of the workforce, medical staff members and vendor communicating information through text messaging about a facility patient or confidential or proprietary business information.

II. PURPOSE:

The purpose of this policy is to establish a consistent procedure to be followed in circumstances where text messaging is used as a means of business communication to comply with Tenet's Information Privacy and Security Program policies, Tenet's Standard of Conduct, Tenet policies, applicable state privacy laws and federal privacy laws.

III. DEFINITIONS:

A. "**Asset**" means 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.

B. A "**Disclosure**" means the release, transfer, provision of access to, or divulging of information in any other manner outside the facility holding the information.

C. **ELECTRONIC PROTECTED HEALTH INFORMATION** or **ePHI** means protected Health Information that is created, received, maintained, or transmitted in electronic form by or on behalf of a covered entity.

D. "**Health Information**" is broadly defined and includes any health information that pertains to a particular patient.

E. "**Personal Portable Electronic Communication Devices**" or "**PECD**" includes standard cellular phones, PDA/Smartphones (iPhones, Blackberry, Androids, etc.). Broadband access cards (laptop wireless connectors/air-cards) and numeric and alpha-numeric pager devices.

F. "**Personally Identifiable Information**" or "**PII**" means any information about an individual maintained by **[Facility Name]**, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, education, financial, and employment information.

G. "**Protected Health Information**" or "**PHI**" means any data or information whether oral or recorded in any form or medium, that is created, in the custody of the facility or received by the facility from a health plan, public health authority, employer, life insurer, school or university or health care clearinghouse and related to the past, present or future physical or mental health or condition of an individual, or the past, present or future payment for the provision of health care to the individual. PHI excludes individually identifiable health information 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.

H. "**Secure Texting**" Any messaging occurring inside a Tenet approved encryption application.

I. "**Sensitive/Proprietary Information**" 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.

J. "**Text Messaging**" or "**Texting**" is the act of composing and sending brief, electronic messages between two or more mobile phones, or fixed or portable devices over a cellular or Wi-Fi network. It also includes sending message from mobile carrier websites and web-based paging applications. MMS Messages are messages that contain images, video and sound content.

K. "**Unsecured Texting**" Any messaging occurring outside of a Tenet approved encryption application.

L. "**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 of an employee, agent or contractor of a Business Associate.

IV. POLICY:

Effective security of confidential, proprietary and/or protected health information communicated electronically is a team effort, involving the participation and support of every facility workforce member and affiliate, who would be a user of the facility's confidential, proprietary and/or protected health information. The policy shall be applied in **[Facility Name]** to allow secured texting through the Tenet approved application.

IV. PROCEDURE:

A. All users must receive approval to use secured text messaging for any business purpose involving confidential or proprietary information.

1. Define facility authorized users:

   a. Administrators and administrative staff

   b. Facility department leaders

   c. Department staff (consider using job titles/positions to identify authorized users)

   d. Medical staff members.

B. **[Facility Name]** Information Services Director, or their designee, shall:

1. Utilize eID provisioning to identify and approve authorized users.

2. Maintain the facility list of all active users and any mobile devices identified by the user on which the secured texting application will be installed for use (whether facility-owned or personal devices). The list will include at a minimum:

   a. Name of approved user;

   b. Title

   c. Mobile device number, facility or personally owned;

   d. Department and;

   e. Approving Supervisor or Approving Sponsor.

f. Evidence of an employee agreement to follow the Text Messaging policy and department procedures.

3. Medical Staff Services will manage the agreement with physicians regarding consent and obligations.

4. Management of PECDs utilized for text messaging

a. All PECDs must be password protected, encryption enabled and with the current Tenet approved mobile device management solution security measures installed.

b. In the event a PECD is incapable of encryption, the device must not be used to communicate any Confidential or Proprietary Information for business purposes.

c. Facility owned PECDs that are used to send text messages containing EPHI shall be wiped clean by Information Systems in coordination with the approving department upon retirement of the devices.

d. Personal PECDs that are used to send text messages containing EPHI shall be wiped clean of all facility related communications, including but not limited to texts, images, notes and any other media containing facility business information used in the employee's role, by Information Systems in coordination with the approving department upon retirement of the devices or no later than the employees' last day of work.

C. Training

1. On-line Training. Participation in on-line training sessions must be documented and maintained in Tenet's online education system.

2. Training materials shall be maintained according to Administrative policy AD 1.11 Records Management and its Record Retention Schedule.

3. Training completion documentation will include the time, date, place and content of each training session, as well as the Workforce members who attended each training session. **[Facility Name]** will maintain such

documentation and make it available for inspection by regulatory authorities, as appropriate.

D. Mitigation

Information regarding any violation discovered by any member of Tenet's Workforce must be reported promptly to the Privacy Security Compliance Officer or a member of the Privacy Incident Response Team (PIRT). The Privacy Security Compliance Officer will be responsible for overseeing the investigation of all reported violations and/or allegations.

A patient, visitor or other individual may report to any member of the Tenet workforce all alleged or known instances of the use and/or disclosure of PHI or other confidential information in violation of the Program.

The Tenet Facility's Compliance Committee and PIRT will mitigate, to the extent practicable, any harmful effect that is known to have occurred as a result of a use or disclosure of PHI, other confidential information or violation of a patient's rights with respect to his/her PHI.

E. Responsible Persons

Responsibility for the content and administration of the Information Privacy and Security Program resides with **[Facility Name]** Hospital Compliance Committee.

F. Enforcement

All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy will be subject to appropriate performance management pursuant to all applicable policies and procedures, up to and including termination. Such performance management may also include modification of compensation, including any merit or discretionary compensation awards, as allowed by applicable law.

V. REFERENCES:

- Tenet Information Privacy and Security Policies and Standards

VI. ATTACHMENTS:

- Attachment A: Employee Request to Utilize Text Messaging
- Attachment B: Information Privacy and Security Attestation