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:

The purpose of the standard is to establish a consistent procedure to be followed in circumstances where corrective, remedial, or disciplinary action is appropriate to address an employee or contractor’s failure to comply with Tenet’s Information Privacy and Security Program policies, Tenet’s Standards of Conduct, applicable state privacy laws and federal privacy laws. These guidelines were designed to align a “typical” privacy violation with the “normal” disciplinary action consequences. These Disciplinary Guidelines are to be used in correlation with Tenet Policies HR.ERW.14 Corrective, Remedial and Disciplinary Action for Violation of Compliance Standards, and HR.ERW.12 Employee Performance Management.

III. DEFINITIONS:

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

IV. STANDARD:

A. Tenet Facilities are strongly committed to the protection of the PHI of all patients throughout the organization. Leadership and employees are reminded that the unauthorized release or unauthorized access of PHI in any form may result in disciplinary action up to and including termination.

B. Any reported or suspected privacy violations will be investigated in accordance with organizational practices. Leadership will be expected to consult with the Chief Human Resources Officer, or designee, and the Privacy and Security Compliance Officer or designee, regarding violations of Tenet’s privacy policies, state privacy laws, or federal privacy laws.

C. When extenuating circumstances exist or atypical violations occur, the facility Chief Human Resources Officer, or designee, and the employee’s Manager, in consultation with the Privacy and Security Compliance Officer are to rely on their best judgment in determining the appropriate disciplinary action consistent with Tenet’s Progressive Discipline Principles and in consideration of an employee’s past disciplinary history.
D. The Facility will normally follow progressive discipline; however, depending on the circumstances and on the severity of the violation, an employee may be disciplined at any level of the disciplinary process up to and including termination of employment.

E. For employees covered by a collective bargaining agreement (CBA), the facility Chief Human Resources Officer or equivalent must consult the CBA in administering these guidelines and seek assistance from Tenet Labor Relations as appropriate.

F. Types of Disciplinary Action
   1. Verbal Counseling/Coaching
   2. Verbal Counseling/Written
   3. Written Warning
   4. Final Written Decision Making Leave/Suspension
   6. Termination

G. Severity Level of Privacy Violations

It is recognized that there are different severity levels of privacy violations related to the unauthorized release, or access to PHI. This standard outlines those levels. The examples provided below are not exhaustive, but are intended to be an informational guide for Leadership, Supervisors, and Human Resources in order to make the best decision when administering the disciplinary action. This standard does not alter the ‘at-will’ employment relationship and either the employee or the organization may terminate the employment relationship at any time, with or without notice and with or without cause.

1. Severity Level I
   a) A Level I violation may consist of the following:
      (1) Leaving documents containing PHI in public areas.
      (2) Leaving a computer screen unattended with unsecured PHI in an accessible area.
      (3) Discussing PHI in public areas with colleagues involved in treatment, payment or operations of a patient in a volume higher than necessary without considering the surroundings.
(4) Discarding PHI into the trash instead of a secure shred container.

(5) Authorized texting patient identifiable information, images, or PHI of a patient to an unauthorized party.

(6) Any other violation with similar scope that may result from unintentional error or oversight.

b) A Level I violation may result in a verbal warning/coaching and may be documented on a performance improvement plan to be included in the employee’s personnel file. If the disciplinary action was a verbal coaching session, then “coaching” is to be written at the top left of the Performance Management for.

2. Severity Level II

a) A Level II violation may consist of the following:

(1) Transmitting PHI via mail, facsimile or electronic mail to the incorrect location/recipient. (eg. Inadvertent fax of PHI to the incorrect recipient by misdialing (manual) or mistyping (electronic) the fax number.)

(2) Accidental electronic transfer/e-mail of patient data to unintended vendors that are not contracted as business associates of the entity.

(3) Employee use of work credentials in order to access, view or retrieve Protected Health Information via Cerner, HPF or any other electronic systems for personal use (anything other than a business purpose), or otherwise required by their designated work role or state/federal law.

(4) Entering information into the patient’s account/medical record for the wrong patient that results in an individual, a doctor’s office, a business associate, etc. receiving the incorrect patient information.

(5) Allowing a co-worker to use your workstation/log-in credentials to access a patient’s medical record, sharing passwords or other log-in credentials (intent to circumvent information security/patient safety efforts).

(6) Employee accessing paper or electronic medical record of a
family member or friend to print their results for them instead of the patient signing a release authorization in medical records.

(7) Inadvertent disclosure of PHI to the incorrect patient by not double-checking each page and/or using patient identifiers (i.e. discharge instruction).

(8) Discussing PHI with colleagues or vendors that do not have the need to know the patient’s information.

(9) Discussing PHI with family or visitors of the patient without first allowing the patient an opportunity to exercise their right to consent or object to their information being disclosed.

(10) Any other violation with similar scope that may involve access to or release of PHI.

b) Loss of paper records, laptop, computer, blackberry, iPhone, iPad, flash drive, unsecured assets or any electronic device that contains PHI.

(1) A repeated Level I violation.

c) A Level II violation may result in a written warning and will be documented on a performance improvement plan.

3. Severity Level III

a) A Level III violation may consist of the following:

(1) Employee accessing an electronic medical record of a patient (e.g., family, friend, or VIP patient) when they are not a member of the treatment team, do not have an operational purpose for the access, or are not tasked with billing or coding actions (e.g. snooping).

(2) Knowingly and intentionally releasing PHI, in any form, of a patient to unauthorized individuals without authorized consent of the patient.

(3) Intentionally releasing components of the medical record including prescriptions of one patient to another patient. Or to the non-intended recipient.

(4) Posting patient information, images, or PHI of a patient on
social media web sites (see also Tenet Standards of Conduct).

(5) Any other violation with similar scope that may involve access to or release of PHI.

(6) A repeated Level II violation.

b) A Level III violation may result in a final written warning and a three-day suspension without pay.

4. Severity Level IV

a) A Level IV violation may consist of the following:

(1) Intent of personal gain by accessing medical records, whether paper or electronic medical record of a patient, family member, co-worker’s or other member of the public.

(2) Selling, releasing, or otherwise disclosing for personal gain, or with malicious intent.

(3) Access of PHI to compile a mailing list for personal use or to sell.

(4) Taking a laptop or patient file that contains PHI for personal use or to sell.

(5) Employee theft of any Tenet asset that contains PHI (e.g. paper or electronic media laptops, computers, or any electronic device).

(6) Unauthorized texting patient identifiable information, images, or PHI of a patient intentionally to an unauthorized party.

(7) Any other violation with similar scope that may involve access to or release of PHI.

(8) A repeated Level III violation.

b) A Level IV violation may result in immediate termination of employment, and may result in civil or criminal penalties initiated by the organization or an external agency.

H. Additional Consideration(s)

1. To determine the severity of a privacy incident and the appropriate disciplinary
action, facility Leadership, Supervisor, Regional Privacy Officer, or the
Hospital Compliance Officer in the absence of a Regional Privacy Officer, and
the Human Resources Department will take into consideration the answers to
the following questions:

a) Is this a repeat occurrence for this employee?

b) Did the employee complete privacy training within the last year?

c) Was the violation intentional or accidental?

d) Did the employee fail to self-disclose?

e) Does this employee have other documented performance issues?

I. Performance Management Process

1. Depending on the severity, a breach may result in mandatory re-education,
suspension and/or termination of employment, reporting to authorities, and
reporting to applicable licensing/certification and registration agencies.

2. The Facility Human Resources department will provide assistance, guidance,
and support to Leadership, Supervisors and Employees in all aspects of the
Performance Management process.

3. The facility Supervisor in consultation with the Human Resources
Department is responsible for ensuring that Tenet’s disciplinary and remedial
policies are enforced consistently for all employees involved in or responsible
for a violation.

J. IMPLEMENTATION:

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

1. Tenet Facility Leadership

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 Regional Privacy Officer.

2. Corporate Office

Tenet’s Information Privacy and Security Office, through the Privacy and Security Compliance Officers, will work with the Tenet Facility Information Security Officers 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.

K. REFERENCES:

~ EC.PS.01.00 Information Privacy and Security Administration Policy

~ EC.PS.01.00 Information Privacy and Security Administration Policy, Attachment A – Glossary of Definitions.

~ EC.PS.02.00 Patient Information Privacy Policy

~ EC.PS.03.00 Patient Rights Policy

~ EC.PS.04.00 Information Security Policy

~ HR.ERW.12 Employee Performance Management

~ HR.ERW.14 Corrective, Remedial and Disciplinary Action for Violation of Compliance Standards

~ HR.ERW.15 Ethics and Compliance Training

L. ATTACHMENTS:

~ Attachment A: Sample Recommended Disciplinary Action Scenarios
SAMPLE RECOMMENDED DISCIPLINARY ACTION SCENARIOS:

You work in Patient Access and know that an adult member of your family (e.g. your spouse and/or adult child) visited the Emergency Department. Curious about your relative’s diagnosis and treatment, you access their PHI using the electronic medical record system.  
**Severity: Level III May result in a final written warning and a three day suspension without pay.**

You receive a call from a physician’s office stating that the office just received a fax from your department containing information of a patient that is not their patient.  
**Severity: Level II May result in a written warning and documented on a performance improvement plan.**

You work in the business office and you receive a call from a patient stating that they not only received their bill, but also the bill of another patient. The bill contains medical information as well as patient account information.  
**Severity: Level II May result in a written warning and documented on a performance plan.**

You are a nurse and a patient comes to you upset and alleges that another nurse on your floor has inappropriately gossiped about the patient’s substance abuse treatment with another nurse.  
**Severity: Level I May result in a verbal warning/coaching may be documented in personnel file.**

You are contacted by a patient who states they were recently discharged from the hospital and when they arrived home they noticed the nurse provided them with another patient’s discharge instructions.  
**Severity: Level II May result in a written warning and documented on a performance plan.**

You notice a note on your manager’s desk from a coworker requesting time-off for a medical procedure. As to relieve your co-worker’s anxiety about the pending exam you access her medical record to ensure she is okay. Relieved that it was nothing serious you tell your coworkers about the procedure and that there is nothing for them to worry about.  
**Severity: Level III May result in a final written warning and a three day suspension without pay.**

You are related to a patient that has expired in the ER. You do not work in ER, but have access to HPF. You access HPF documents, including physician notes, copy them and give to an attorney looking for evidence of malpractice.  
**Severity: Level IV May result in immediate termination of employment.**

A family member of an employee needs his son’s immunization history before he can attend school. He appeals to you to look it up. You search the medical record to get the information.  
**Severity: Level II May result in a written warning and documented on a performance plan**

You leave a hard copy or electronic screen shot of patient information in an area which is readily accessible for review by unauthorized personnel, patients or the public (assuming no one saw the PHI).
Severity: Level I May result in a verbal warning/coaching may be documented in personnel file.

You share information on a patient’s medical condition, room location, family contacts or personal history with unauthorized personnel, the public, the press or investigative personnel.

Severity: Level IV May result in immediate termination of employment.