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 this Standard is to comply with the Privacy Rule which requires covered entities to limit uses and disclosures of, and requests for, protected health information to “the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”

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:

Workforce members and Business Associates acting on behalf of Tenet must use only the minimum amount of information necessary to accomplish the intended purpose of the access, use, and/or disclosure of PHI.

Tenet will use and/or disclose PHI as outlined in EC.PS.02.00 Patient Information Privacy Policy and as follows:

A. Minimum Necessary

The Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This includes oral, written or electronic information that is used in treatment, payment or healthcare operations.

1. Limited Data Set

   A limited data set excludes the following direct identifiers of the individuals and their relatives, household members, and employers:

   a. Names;
   
   b. Postal address information, other than town or city, State, and zip code;
<table>
<thead>
<tr>
<th>Title:</th>
<th>Page: 5 of 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>USES, DISCLOSURES, AND</td>
<td></td>
</tr>
<tr>
<td>MINIMUM NECESSARY STANDARD</td>
<td></td>
</tr>
</tbody>
</table>

- c. Telephone numbers;
- d. Fax numbers;
- e. Electronic mail addresses;
- f. Social security numbers;
- g. Medical record numbers;
- h. Health plan beneficiary numbers;
- i. Account numbers;
- j. Certificate/license numbers;
- k. Vehicle identifiers and serial numbers, including license plate numbers;
- l. Device identifiers and serial numbers;
- m. Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers;
- n. Biometric identifiers, including finger and voice prints; and
- o. Full face photographic images and any comparable images.

2. Exceptions to Minimum Necessary:

The Privacy Rule outlines situations in which the minimum necessary rule does not apply. Members of Tenet’s Workforce must only use, disclose or request the minimum necessary amount of PHI in all situations, except the following:

- a. Disclosures to or requests by a Health Care Provider for Treatment.
- b. Uses or disclosures made to the patient or the patient’s personal representative.
- c. Uses or disclosures pursuant to and consistent with the terms of a valid patient authorization.
- d. Disclosures to the Director of the Office for Civil Rights of the U.S. Department of Health and Human Services (“HHS”) for HIPAA compliance purposes.
e. Uses or disclosures that are required by law (i.e., a mandate that is contained in law that compels the organization to use or disclose PHI and that is enforceable in a court of law; e.g., court orders, court-ordered subpoenas, civil or authorized investigative demands, Medicare conditions of participation).

f. Uses or disclosures that are required for compliance with the regulations implementing the other administrative simplification provisions of HIPAA (i.e., the transactions and code sets standard, security standard, etc.).

3. System Access

Minimum necessary will be supported through authorization, access, and audit controls (e.g., roles-based access) and should be implemented for all systems that contain identifiable patient information. Within the permitted access, an individual system user is only to access what they need to perform his or her job functions. Users are prohibited from utilizing their user credentials in order to access electronic systems to review or retrieve their electronic medical record, as well as those of their family and friends. This practice is considered personal use and an activity outside of business related purposes.

B. Access to and Uses of PHI

The Privacy Rule requires covered entities to identify workforce members who need access to PHI, to identify the categories and conditions of such access, and to make reasonable efforts to limit access consistent with such policies.

Following are steps that shall be taken by Tenet Facilities to implement the minimum necessary standard with respect to the use of PHI by members of Tenet’s Workforce and Tenet’s Business Associates:

1. Persons (or classes of persons) within the organization who need access to PHI to carry out their duties shall be identified. This information shall be documented on Attachment A and reviewed on a periodic basis, no less than annually.

   a. Consider the following roles: persons who treat patients; billers; appointment scheduling clerks; medical records staff; receptionists. Review job descriptions to determine specific PHI data elements that particular workforce members may require to carry out their duties.

2. With respect to each person (or classes of persons), steps shall be taken to identify the category (or categories) of PHI to which access is needed and any
conditions appropriate to such access. This information shall be documented on Attachment A and reviewed on a periodic basis.

a. Consider the following categories of PHI and roles: Entire medical record-persons who treat patients; medical records staff; Summary or face sheet-appointment scheduling clerks, receptionists.

b. Once persons (or classes of persons) who need access to PHI and categories of information are identified, reasonable steps must be taken to limit access of such identified persons only to their respective identified categories of PHI. These steps shall be documented and reviewed on a periodic basis.

c. For computerized medical records systems, create access roles for only identified persons and identified categories of PHI. For paper records, the medical records staff or other persons who distribute medical records must monitor access.

d. Need to consider reasonable physical, administrative and technical security controls; i.e., locked file cabinets, secure fax machine, discourage conversations about a patient’s condition in public places, computer passwords, etc.

e. Sign-in sheets are permissible (The Joint Commission (TJC) may want more restrictive exposure such as an individual sheet or label per patient). Discussions over the telephone where persons can hear the conversation should be relatively limited in general. Facility redesign is not necessary.

3. The Privacy Rule requires that covered entities adopt policies and procedures with regard to uses and disclosures that occur routinely. With respect to disclosures of PHI, the covered entity or business associate making the disclosure shall determine what constitutes the minimum necessary.

Following are steps that Tenet Facilities must take to implement the minimum necessary standard with respect to disclosures and requests of PHI made on a routine or recurring basis or on a nonrecurring basis:

a. When a disclosure or request is of the type that occurs on a routine or recurring basis, the Tenet Facility must establish a standard protocol that limits the PHI disclosed or requested to the amount reasonably necessary to achieve the purpose of the disclosure or request. Attachment B to this Standard includes examples of (1) the disclosures and requests that are made on a routine or recurring basis, (2) the purposes of the disclosures or requests, (3) the criteria established to limit the PHI disclosures or
requests to that which is reasonably necessary for the purpose of the disclosures or requests. Each Tenet Facility must create and regularly review and update an Attachment B to its standard protocol.

(1) The Tenet Facility must identify which disclosures or requests occur on a routine or nonrecurring basis. For instance, for billing purposes, the protocol may be to disclose only records for service at issue. For outside billers, the protocol may be to disclose only that portion of the medical record that the biller needs to prepare the bill. The protocols must be concise. See the examples in Attachment B.

b. For any non-routine disclosure or request the Tenet Facility must:

(1) Develop criteria to limit the PHI disclosed or requested to the amount reasonably necessary to accomplish the purpose of the disclosure or request; and

(2) Train designated staff administrators to review Workforce requests to disclose or request such PHI on an individual basis in accordance with such criteria.

(a) Appropriate criteria may include:

(i) The purpose of the request or disclosure

(ii) The nature and extent of information requested

(iii) The extent to which requested PHI can be extracted from the rest of the medical record without undue burden and without viewing unnecessary parts of the record

(iv) Where the PHI will be viewed or used

(v) The availability of physical, technical and other security measures at the place of viewing or use

(vi) The immediacy or urgency of the need for the requested PHI

(vii) The trustworthiness of the person who will access or use the PHI
C. Responding To Requests For Disclosure

The Privacy Rule requires that covered entities consider the feasibility of utilizing the limited data set in complying with the minimum necessary requirements of the Privacy Rule. However, the Privacy Rule also permits a covered entity to employ its traditional minimum necessary policies and procedures if it decides that the limited data set will not meet the needs of the particular use, disclosure, or request in question.

Tenet staff may rely on a requested disclosure as representing the minimum necessary for the stated purpose (if reliance is reasonable under the circumstances) in the following situations:

1. When making disclosures to public officials and the requesting official represents that the information requested is the minimum necessary for the stated purpose.

2. When the information is requested by another covered entity.

3. When the information is requested by a health care professional (e.g., a physician or nurse) who is a member of the Tenet Facility’s Workforce or is a Business Associate of Tenet for the purpose of providing professional services to Tenet, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).

4. When the information is requested for research purposes and the person requesting the information has provided documentation or representations that comply with Patient Information Privacy Policy.

D. Incidental Uses Or Disclosures

An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as by-product of an otherwise permitted use or disclosure. Examples of incidental uses or disclosures include: (1) Utilizing patient sign-in sheets or calling out a patient’s name in a waiting room, as long as the information disclosed is appropriately limited; and (2) Discussing laboratory results with a patient in a joint treatment room.

The Privacy Rule requires that covered entities reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. Accordingly, Tenet should determine risk areas for violation of these provisions and put in place measures to limit incidental disclosures. Incidental uses and disclosures are not required to be part of an accounting under EC.PS.02.00 Patient Information Privacy Policy.
E. Patient Authorization

1. Tenet may use and disclose PHI without an individual’s authorization as outlined in EC.PS.02.00 Patient Information Privacy Policy.

2. Tenet must obtain patient authorizations to use or disclose PHI for a purpose other than providing Treatment, obtaining Payment, carrying out its Health Care Operations (TPO), or making a disclosure based on public policy pursuant to EC.PS.02.03 Public Interest and Benefit Activities Standard, or except as otherwise provided in EC.PS.02.00 Patient Information Privacy Policy.

   a. A valid authorization must contain at least the following elements and statements (see Attachment C for a sample form):

      (1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

      (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

      (3) The name or other specific identification of the person(s), or class of persons, to whom the Tenet Facility may make the requested use or disclosure;

      (4) A description of each purpose of the requested use or disclosure. “At the request of the individual” is sufficient when the individual initiates the authorization;

      (5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. “End of research study,” “none,” or similar language is sufficient if the authorization is for use or disclosure of PHI for research;

      (6) A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke and a description of how the individual may revoke the authorization or a reference to the Tenet Facility’s Notice of Privacy Practices for further instructions;

      (7) A statement that the provision of treatment and payment may not be conditioned on obtaining this authorization unless otherwise allowed (e.g., research related treatment);
A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;

A statement that the individual may inspect or copy the PHI to be used or disclosed in response to the authorization;

If the use or disclosure of the requested information will result in any direct or indirect remuneration to the Tenet Facility from a third party, a statement that such remuneration will result;

If a Tenet Facility seeks an authorization from an individual for their own use or disclosure of PHI, the Tenet Facility must provide the individual with a copy of the signed authorization; and

The signature of the individual and date. If the authorization is signed by a personal representative (as defined by state law) of the individual, a description of such representative's authority to act for the individual.

b. The authorization must be written in plain language.

F. Documentation

Documentation shall be maintained in accordance with Administrative Policy AD 1.11 Records Management and its Record Retention Schedule.

V. IMPLEMENTATION:

A. Facility

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.

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;

c. Report monitoring activity to the Privacy and Security Compliance Officer

B. Corporate Office

1. Tenet’s Corporate Privacy/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 Committees 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.02.03 Public Interest and Benefit Activities Standard
- EC.PS.01.00 Information Privacy and Security Administration Policy, Attachment A – Glossary of Definitions
- EC.PS.04.02 User Security and Conduct Standard
- Administrative policy AD 1.11 Records Management and its Record Retention Schedule
- 45 C.F.R. Parts 160 and 164

VII. ATTACHMENTS:

- Attachment A: Sample Routine and Recurring Access
- Attachment B: Example of Protocols for Routine or Recurring Disclosures or Requests
- Attachment C: Sample Authorization to Use and Disclose Health Information