I. PURPOSE:

The purpose of this standard is to ensure that affected individuals, the media, and the Secretary of Health and Human Services (HHS) are appropriately notified of any Breach of unsecured protected health information (PHI) in accordance with the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), Breach Notification Rule, FTC Health Breach Notification Rule and all applicable regulations and guidance.

II. DEFINITIONS:

A. “Breach” means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

B. “Breach Notification Rule” means the HIPAA privacy regulations set forth at 45 CFR part 164, Subpart D.

C. “Disclosure” means the release, transfer, provision of access to, or divulging of information in any other manner by the Tenet Facility holding the information.

D. “Privacy Rule” means the HIPAA privacy regulations set forth at 45 CFR part 164, Subpart E, and as further described in Tenet’s Privacy and Security Policies.

E. “Protected Health Information” or “PHI” means individually identifiable health information that is transmitted by electronic media; maintained in any medium as described in the definition of electronic media; or transmitted or maintained in any other form. 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.

F. “Unsecured Protected Health Information” or “Unsecured PHI” means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5. Redaction is not an approved method of destruction.

G. “Use” means the sharing, utilization, examination, or analysis of PHI within an entity that maintains PHI.
H. Additional capitalized terms used herein are defined in the Information Privacy and Security Glossary of Definitions.

III. STANDARD:

Tenet will notify affected individuals, HHS, and the media, where required, of any Breach of unsecured protected health information that compromises the security or privacy of the protected health information. All suspected Breaches of unsecured PHI will be investigated, and all necessary notifications will be sent, in accordance with the guidelines set forth in this standard.

A. Breach Determination

To determine whether an incident constitutes a Breach under this standard, follow the steps below.

Step 1: Is the PHI “Unsecured?”

The Breach notification requirements only apply to “unsecured” PHI. If the PHI involved in the alleged Breach does not meet the definition of “Unsecured Protected Health Information” described in Section II. F, the incident is not a Breach, and the notification requirements set forth in this policy do not apply. Review any state notification or other compliance requirements for applicability.

Step 2: Does an exception apply?

Determine whether the incident meets one of the following exceptions to the definition of “Breach.”

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a Business Associate, if such acquisition, access, or use of PHI was made in good faith and within the scope of authority and does not result in further use or disclosure of PHI in a manner not permitted under the Privacy Rule.

2. Any inadvertent disclosure of PHI by a person who is authorized to access PHI at a covered entity or Business Associate to another person authorized to access PHI at the same covered entity or Business Associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a covered entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure of PHI was made would not reasonably have been able to retain such information.

Step 3: Is there a low probability that the PHI was compromised?

Except as described in Step 2, an acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment based on at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure of PHI was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

B. Notification

Once a Breach has been discovered, Tenet will notify the affected individual(s), the Secretary of HHS, and the media, as applicable, per the requirements set forth below.

1. Notification to Affected Individuals

Following the discovery of a Breach of Unsecured PHI, Tenet will notify each individual whose Unsecured PHI has been, or is reasonably believed by Tenet to have been accessed, acquired, used, or disclosed as a result of such Breach.

a. Actual Notice—The notification will be in writing and sent via First Class mail to the individual at his or her last known address. Notice may be given by electronic mail, if the individual has agreed to such method in advance.

Substitute Notice—If there is insufficient or out-of-date contact information that precludes written notification to the individual, a
substitute form of notice reasonably calculated to reach the individual shall be provided.

(1) If there is insufficient contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(2) If there is insufficient contact information for 10 or more individuals, then such substitute notice shall be in the form of either: (i) a posting on the Tenet Entity’s website for a period of 90 days or, (ii) conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside. Both methods must include a toll-free number that remains active for at least 90 days. Do not contact the media without clearance from Corporate Communications and Tenet’s Information Privacy and Security Office.

b. Urgent Situations—In any case deemed urgent by Tenet because of possible imminent misuse of Unsecured PHI, Tenet may provide information to individuals by telephone or other means, as appropriate, in addition to the general requirement to send actual or substitute notice.

c. Timing—Notification must be provided without unreasonable delay, and in no case later than 60 calendar days after discovery of a Breach. A Breach is considered to be “discovered” by a covered entity as of the first day on which such Breach is known to the covered entity (or the covered entity’s employee), or, by exercising reasonable diligence would have been known to the covered entity (or its employee).

d. Content—All notifications to individuals must contain, to the extent possible, the following elements:

(1) A brief description of what happened, including the date of the Breach and the date of discovery;

(2) A description of the types of Unsecured PHI that were involved in the Breach;
Any steps the individuals should take to protect themselves from potential harm;

A brief description of what Tenet is doing to investigate the Breach, mitigate the harm, and protect against future Breaches; and

Procedures for individuals contact Tenet to ask questions.

Refer to Attachment C and Attachment D for template Notification to Individual Letters.

2. Notification to Health and Human Services

b. Breaches involving less than 500—For Breaches involving less than 500 individuals, Tenet Entities will provide notice to HHS at the same time notice is provided to the affected individuals. Such notice is to be provided to HHS in the manner specified on the HHS website.

c. Breaches involving 500 or more—For Breaches involving 500 or more individuals, Tenet will provide notice to HHS at the same time notice is provided to the affected individuals. Such notice is to be provided to HHS in the manner specified on the HHS website. Consult with Tenet’s Privacy and Security Office before making an HHS notice required under this section.

3. Notification to the Media

Tenet must notify prominent media outlets if a Breach of Unsecured PHI involves more than 500 individuals of a State or jurisdiction. The content of the notice shall include the elements described in Section B.1.e above. Contact the Tenet Facility’s Corporate Communications liaison and Tenet’s Privacy and Security Office prior to notifying any media outlet of such a Breach.

4. Law Enforcement Delay—if a law enforcement official communicates to Tenet that a notification or posting otherwise required by this standard would impede an investigation, Tenet shall delay such notification as follows:

a. If the communication from the law enforcement official is in writing and specifies the time for which a delay is required, Tenet
shall delay the notification in accordance with the written communication.

b. If the communication is made orally, Tenet shall document the communication (including the identity of the official), and delay the notification no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

c. The notification(s) must be made no later than 15 business days after the date designated as the end of the law enforcement delay.

B. Business Associates

1. Notification from Business Associates—following the discovery of a potential Breach, Tenet Business Associates must notify Tenet of such Breach without unreasonable delay, and in no event later than 60 calendar days after discovery of the potential Breach. Tenet’s Business Associate Agreements may specify a specific time frame and procedure for notifying Tenet of potential breaches.

2. For purposes of Tenet’s timely notification of affected individuals:

a. If the Business Associate is acting as Tenet’s agent (e.g., Conifer), the Business Associates’ discovery of the Breach is imputed to Tenet; therefore, Tenet’s timeline for notification purposes begins when the Business Associate discovers the Breach.

b. If the Business Associate is an independent contractor, Tenet “discovers” the Breach at the time that the Business Associate notifies Tenet of the Breach.

3. Content—the notification from the Business Associate must include, to the extent possible, (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach; and (ii) any other available information that Tenet is required to include in notification to the affected individual(s).

C. Impact on State Law Notification Requirements
1. General Rule: This standard preempts any contrary state law regarding Breach notification requirements. A state law is “contrary” if:
   
a. a covered entity could find it impossible to comply with both the state and federal requirements, or
   
b. the state law stands as an obstacle to the accomplishment and execution of the full purpose and objectives of the Breach notification requirements.

2. It is not anticipated that the federal notification requirements set forth in this standard will often preempt state notification laws. Therefore, each potential Breach must be analyzed to determine the applicability of state privacy notification laws as well as state identity theft notification statutes. To the extent that all state and federal statutory requirements (content and timing) can be accommodated, Tenet Entities may send one combined notice to affected individuals.

D. Documentation Requirements

It is Tenet’s burden to prove that all required notifications under this standard have been made. To that end, Tenet Facility Compliance Officers and/or Regional Privacy Officers must thoroughly and timely document:

1. The investigation of the incident in Compliance Central. See Attachment A for an investigation tool.

2. The risk assessment used to determine whether or not the Breach posed a significant risk of harm to the individual. See the Risk Assessment tool set forth in Attachment B.

3. Any and all analysis and steps taken to determine whether or not a Breach occurred.

IV. IMPLEMENTATION:

A. Tenet Facility WITHOUT Regional Privacy Officer

1. The Tenet Facility Compliance Officer, Tenet Facility Information Security Officer and the 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; 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 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; and
      c. Report monitoring activity to the Regional Privacy Officer.

C. Home Office

   1. Tenet’s Information Privacy/Security Office must work with the Tenet Facility COs, Tenet Facility PIRTs and Tenet Facility Compliance Committees to develop, maintain, and update procedures and standards for protecting the privacy of PHI and affording patients their rights with respect to their PHI.

   2. Tenet Home Office and Tenet Regional Offices must incorporate these standards into their specific policies and procedures where necessary.

V. REFERENCES:
- EC.PS.01.00 Information Privacy and Security Administration Policy

- EC.PS.01.01 Information Privacy and Security Incident Handling Standard

- Information Privacy and Security Glossary of Definitions

- 45 C.F.R. Parts 160 and 164

- Guidance Specifying Technologies and Methodologies that render PHI “Secured,” 74 Federal Register 19006 (April 27, 2009)

VI. ATTACHMENTS:

- Attachment A: Breach Investigation Tool

- Attachment B: Breach Risk Assessment

- Attachment C: Template Notification Letter to Individual: Non-California

- Attachment D: Template Notification Letter to Individual: California
Breach Investigation Tool

**Breach Investigation:**

1. How was the potential breach brought to your attention:

2. What date was the potential breach “discovered” and by whom?

3. Briefly describe what was reported to you:

4. Provide the name(s) of any individuals you interviewed regarding the potential breach:

5. Provide any additional information learned from the interviews:

6. Does law enforcement need to be notified (Yes or No)? If Yes, provide the date of notification, the contact name and the name of the agency:

7. If applicable, identify the hospital data system(s) that was involved in the breach and pull audit trail(s) if available. Consult with Tenet IS as necessary. Identify the person reviewing the audit trail(s):

8. How many individuals are affected by this breach?

9. Was the acquisition, access, use or disclosure of PHI by a member of the hospital’s or a Business Associate’s workforce or a person acting under the authority of the hospital or Business associate? (Yes or No)

10. Was the acquisition, access or use unintentional? (Yes or No)
**Breach Investigation Tool**

11. Was the acquisition, access or use in good faith? (Yes or No)

12. Was the acquisition, access or use within that person's scope of authority? (Yes or No)

13. Is there a “good faith” belief that the unauthorized person who received the PHI would not reasonably have been able to retain the PHI? (Yes or No)

14. If the PHI was disclosed, what is the name of the individual(s) or entity(s) who received the PHI?

15. Was the PHI further used or disclosed in an impermissible manner by the recipient? (Yes or No)

16. If the PHI was further disclosed, what is the name of the individual(s) or entity(s) who received the PHI?

17. Was the PHI retrieved from the recipient? (Yes or No)

18. If the PHI was not retrieved from the recipient, did the recipient destroy the PHI or provide satisfactory assurances that the PHI will not be further used or disclosed? (Yes or No)

**Resolution and Corrective Actions:**

Develop corrective actions and determine what can be done to prevent future occurrences.

1. Identify the step taken to correct any system issues (e.g., disable auto-printing or auto-faxing, update the system with the correct contact information, etc.):

2. Review user security access levels for appropriateness and identify any changes made:

3. Discuss the results with the manager or supervisor of the department where the breach occurred and identity any changes to improve the process or procedure to prevent future occurrences:
**Breach Investigation Tool**

4. List all policy or procedures that will be changed or updated:

   ___________________________________________________________

   ___________________________________________________________

5. Always retrieve the PHI when possible. Send a self-addressed stamped envelope or a courier to the recipient if necessary. If the PHI cannot be retrieved document the recipient’s assurances that PHI was not further disclosed, destroyed and their method of destruction:

   ___________________________________________________________

   ___________________________________________________________

6. Provide the date when counseling/education was provided to the erring person or staff members ensuring they understand what they did and why it was wrong:

   ___________________________________________________________

7. Attach any proof of the counseling, sign-in sheets and/or meeting minutes to the Compliance Central incident.

8. If the violation was egregious or if it was deemed intentional you should inform your HRD and A-Team and let them handle any employee sanctions/discipline. Ensure that all employee sanctions/disciplines are documented in the employee’s HR file.

9. Date the disclosure(s) was accounted for:

   ___________________________________________________________

10. If this investigation was raised through an allegation, provide the date and method of the follow-up with the complainant:

    ___________________________________________________________

**HIPAA Breach Notification:**

If the breach poses a significant risk to the individual whose PHI was disclosed please provide appropriate notice of the breach in accordance with the Breach Notification Policy.

**State Security Breach Notification:**

Regardless of whether a breach is in violation of the Privacy Rule or Security Rule there may be reporting obligations under state security breach reporting laws that are not preempted by the Privacy Rule or Security Rule.

As of December 2014, the following states where there are Tenet hospitals have enacted security breach notification laws: **Arizona, California, Florida, Georgia, Illinois, Massachusetts, Missouri, North Carolina, Pennsylvania, South Carolina, Tennessee, and Texas.**
Breach Risk Assessment

An impermissible use or disclosure of protected health information (PHI) is presumed to be a breach unless the covered entity demonstrates that there is a low probability that the information has been compromised. Consequently, breach notification is necessary in all situations unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised.

Summary of Events:

<table>
<thead>
<tr>
<th>Breach Risk Assessment Date of Incident</th>
<th>Number of individuals affected:</th>
</tr>
</thead>
<tbody>
<tr>
<td>What happened?</td>
<td></td>
</tr>
</tbody>
</table>

Breach Determination

To determine whether an incident constitutes a Breach under this Policy, follow the steps below.

Step 1: Is the PHI “Unsecured”? (Yes or No)

The Breach notification requirements only apply to “unsecured” PHI. If the PHI involved in the alleged Breach does not meet the definition of “Unsecured Protected Health Information” described in Section II.F. of the Breach Notification Standard, the incident is not a Breach. Analysis of any state notification or other compliance requirements should still be assessed for applicability.

If answer is No, STOP; this is not a breach.

If the answer is Yes, continue to Step 2.

Step 2: Does an exception apply?

Determine whether the incident meets one of the following exceptions to the definition of “Breach.”

Exception 1: workforce member or business associate:

a. Was unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a Business Associate? (Yes or No)

b. If yes, was acquisition, access, or use was made in good faith and within the scope of authority? (Yes or No)

c. Was the PHI further use or disclosed in a manner not permitted under the Privacy Rule? (Yes or No)

If a=Yes, b=Yes and c=No; the exception is met. Stop; this is not a breach.
Breach Risk Assessment

**Exception 2:** inadvertent disclosure to Hospital Workforce member, business associate or member of the OHCA:

a. Was the inadvertent disclosure by a person who is authorized to access PHI at the facility or business associate? (Yes or No)

b. Was the inadvertent disclosure to another person authorized to access PHI at the same facility or business associate or OHCA in which the covered entity participates? (Yes or No)

c. Was the PHI further use or disclosed in a manner not permitted under the Privacy Rule? (Yes or No)

If a=Yes, b=Yes and c=No; the exception is met. Stop; this is not a breach.

**Exception 3:** is there a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information? (Yes or No)

If Yes; the exception is met. Stop; this is not a breach.

If an exception is not met continue to Step 3.

**Step 3:** Is there a low probability that the PHI has been compromised?

Except as described in Step 2, an acquisition, access, use, or disclosure of unsecured PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the type of PHI (e.g., was it names only, or was it names and social security numbers). Evaluate what type of PHI was potentially compromised, how much was actually disclosed, and the risks associated with the type of information disclosed. For example, if only patients’ names were disclosed, that is less problematic than if the patients’ social security numbers and dates of birth were disclosed.

<table>
<thead>
<tr>
<th>Type of Information disclosed (e.g., names/social security/credit card numbers/clinical information/medical history, etc.):</th>
</tr>
</thead>
</table>

09-03-15
Breach Risk Assessment

2. Who was the disclosure made to, or who used the PHI improperly (e.g., was it an identity thief, or was the wrong info faxed to the wrong doctor). Consider who received the PHI, and the potential associated risks. For example, a misdirected fax to a physician presents significantly different risks that accidentally disclosing a patient’s PHI to his or her employer.

Who received/used the information:

3. Was the PHI actually accessed or viewed, or was only the potential for disclosure an issue. Determine whether the PHI was actually acquired or viewed. For example, if an EOB was mailed to the wrong patient, and it was returned to you unopened, a risk assessment would show that the PHI had not been compromised. However, if the patient received it, opened it, and called you to tell you they got the wrong bill, that PHI had been compromised.

Was the information actually acquired or viewed (explain):

4. Has the risk been mitigated so that the facility is assured the information will not be used? Consider the extent to which the risk to the PHI has been mitigated. In some situations, it is possible to determine that there is little risk that the compromised PHI will be used improperly. For example, if the wrong type of PHI is sent to a business associate or employee and they assure you the PHI was immediately destroyed and will not be used, the likelihood that the PHI will be disclosed is minimal. Or, if the PHI is sent to an unauthorized person, and they return the PHI, depending on the situation, that may be sufficient to prevent improper use of the information.

Has the risk been mitigated so that the entity is assured the information will not be used (and if so, how?):

5. The risk assessment must be thorough, complete, in good faith, and the conclusions have to be reasonable. If it is determined that a breach has occurred, the notification process must begin. If it is determined that no breach has occurred, attach the completed assessment to Compliance Central.

After completing the risk assessment, it has been determined:

- This is a breach requiring notification, and breach requirements will be followed;

-OR-

- This is not a breach and notification is not necessary.
Template Notification Letter to Individual: Non-California

[Date of letter]

VIA CERTIFIED MAIL
[Mr. Ms. Patient Name or Representative]
[Address]
[City, State Zip]

Re: Notice of Breach of Unsecured Personal Health Information Our Reference #
[insert Compliance Central #]

Dear [Mr./Ms. Last Name]:

We regret to inform you that [Facility Name] discovered a breach of your protected health information. [Include a BRIEF description of the incident. For example: “Your discharge papers were accidentally given to another patient.” “Your lab results were mistakenly faxed to an outside business.” “Your medical record was inappropriately accessed by an employee.” Include the date of the breach and the date of discovery.] [Describe what types PHI was involved in the breach. DO NOT INCLUDE THE ACTUAL PHI.]

[Describe what steps individuals should take to protect themselves from potential harm, if any. If the breach involved a financial risk, such as a disclosure of social security numbers, account numbers, credit card numbers, include the FAQs for identity theft/financial risk.]

The protection of patient information is of the utmost importance to [Facility Name], and we take this matter very seriously. To that end, we have [description of (1) action taken to investigate breach; (2) actions taken to mitigate losses; and (3) actions taken to protect against further breaches.]

We offer you our sincere apology for this matter. Should you have any questions about the information contained in this letter, please call me at (###) ###-####.

Sincerely, [Name]
Privacy Officer
Template Notification Letter to Individual: California

[Date of letter]
[Mr. Ms. Patient Name or Representative] [Address]
[City, State Zip]

Re: Notice of Breach of Unsecured Personal Health Information Our Reference # [insert Compliance Central #]

Dear [Mr./Ms. Last Name]:

We regret to inform you that [Facility Name] discovered a breach of your protected health information. [Include a BRIEF description of the incident. For example: “Your discharge papers were accidentally given to another patient.” “Your lab results were mistakenly faxed to an outside business.” “Your medical record was inappropriately accessed by an employee.” Include the date of the breach and the date of discovery.]

[Describe what types PHI was involved in the breach. DO NOT INCLUDE THE ACTUAL PHI.]

[Describe what steps individuals should take to protect themselves from potential harm, if any. If the breach involved a financial risk, such as a disclosure of social security numbers, account numbers, credit card numbers, include the FAQs for identity theft/financial risk.]

The protection of patient information is of the utmost importance to [Facility Name], and we take this matter very seriously. To that end, we have [description of (1) action taken to investigate breach; (2) actions taken to mitigate losses; and (3) actions taken to protect against further breaches.]

Please note that we are required by law to notify the California Department of Public Health of this incident. The Department may conduct an investigation, and you may be contacted by a representative of the Department as part of that investigation.

We offer you our sincere apology for this matter. Should you have any questions about the information contained in this letter, please call me at (###) ###-####.

Sincerely, [Name]

Privacy Officer