BREACH NOTIFICATION

POLICY

In compliance with Section 13402 of the Health Information Technology for Economic and Clinical Health Act, the Board establishes a Breach Notification Policy. This policy explains how the Board will identify when an impermissive or unauthorized access, acquisition, use, or disclosure of the Board's individual protected health information occurred. The policy also explains how the Board will provide notice to affected individuals including the methods and the time for which the Board will provide such notice.

The purpose of this policy is to provide guidance for breach notification by the Board when impermissive or unauthorized access, acquisition, use and/or disclosure of the Board's individual protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

This policy applies to the Board and all employees, trainees and volunteers, who create, receive, maintain, or transmit PHI. This policy also applies to all business units that provide management, administrative, financial, legal, and operational support to or on behalf of the Board.

Historical Resolution Information	Reviewer:
Date **Resolution Number** 1/22/11 01-13-11 6/20/15 06-34-15	Superintendent Director of IT

BREACH NOTIFICATION

PROCEDURE

I. **Discovery of Breach**

A breach shall be treated as discovered by the Board as of the first day on which such breach is known to the Board, or, by exercising reasonable diligence would have been known to the Board (which includes breaches by the Board's business associates). The Board shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Board (determined in accordance with the federal common law of agency). Following the discovery of a potential breach, the Board shall begin an investigation and conduct a risk assessment. As required the Board shall begin the process to notify each individual whose PHI has been, or is reasonably believed by the Board to have been accessed, acquired, used, or disclosed as a result of the breach. The Board shall also begin the process of determining what external notifications are required.

A. **Reporting an Actual or Suspected Use or Disclosure of PHI**

Any actual or suspected use or disclosure of PHI believed to be in violation of the HIPAA Privacy Rules shall be immediately reported to the Privacy Officer.

1. In the event a suspected unauthorized use or disclosure is discovered by a Workforce Member, the Workforce Member shall immediately notify their supervisor, who shall report the incident to the Privacy Officer.
2. The Board's business associates must notify the Board of a breach of unsecured PHI without unreasonable delay, but in no case later than 60 calendar days after the discovery of a breach. Notice shall include the identification of each individual whose unsecured PHI has been or is reasonably believed by the business associate to have been accessed, acquired, or disclosed during the breach. The business associate shall provide the Board at the time of the notification or as information becomes available, with any other information that the Board is required to include in the notification to the individual. The Board shall be responsible for notifying individuals under this policy.
3. In the event the Board receives notification of a suspected use or disclosure of PHI from a business associate, the Privacy Officer shall coordinate with the business associate to ensure that all necessary information regarding the incident and affected individuals is obtained.

II. **Determining Whether a Breach of Unsecured PHI Occurred**

Upon receiving a report of any actual or suspected unauthorized use or disclosure of PHI as described above, the Privacy Officer shall immediately investigate the incident to determine if the incident resulted in a Breach of Unsecured PHI. All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years. This investigation shall include the following steps:

A. Step 1. Determine whether the incident resulted in a violation of the HIPAA Privacy Rules. If yes, then proceed to Step 2. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy.

B. Step 2. Determine whether the incident involved "Unsecured PHI" (as defined below). If yes, then proceed to Step 3. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy. The Board acknowledges that it does not use encryption methods to secure PHI that is stored in electronic form. Thus, all PHI that is maintained electronically is Unsecured PHI.

C. Step 3. Determine whether the incident is excluded from the definition of the term "Breach" (as defined above). If yes, then proceed to Step 4. If no, then no Breach of Unsecured PHI occurred and no notification is required under this Policy.

D. Step 4. Conduct a risk assessment to determine whether the incident poses a significant risk of financial, reputational or other harm to the affected individual, considering the following factors:

1. Who impermissibly used Unsecured PHI or to whom Unsecured PHI was impermissibly disclosed;
2. Whether the immediate mitigation actions taken by the Board in response to the incident eliminated or significantly reduced the risk of harm to the affected individual;
3. Whether Unsecured PHI was returned to the Board without being accessed;
4. The nature, type and amount of Unsecured PHI that was improperly used or disclosed in connection with the incident; and
5. Any other relevant factors regarding the incident.

If, based on the risk assessment, it is determined that the incident does not pose a significant risk of financial, reputational or other harm to the affected individual, the Board, in consultation with legal counsel if appropriate, shall conclude that no Breach of Unsecured PHI has occurred and that no notification is required under this Policy. The Board will document the outcome of the risk assessment process.

III. **Procedure if No Breach of Unsecured PHI Occurred.**

If after completing Steps 1-4 above, the Board determines that the incident did not constitute a Breach of Unsecured PHI, the Board shall document such conclusion and the rationale for such conclusion and shall maintain such documentation and any additional supporting documents for a period of at least six (6) years from the determination.

IV. **Procedure if a Breach of Unsecured PHI Occurred.**

If after completing Steps 1-4 above, the Board determines that a Breach of Unsecured PHI occurred, the Board shall provide notice of the Breach and maintain documentation of such notice as follows:

A. Timeliness of Notification

After risk assessment and determination that breach notification is required, the Board shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach by the Board or the Board's business associate. The Board bears the responsibility to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

B. Delay of Notification Authorized

If a law enforcement official states to the Board or the Board's business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (A) of this section is submitted during that time.

C. Content of Notice

The notice must be written in plain language and contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

D. Methods of Notification

The method of notification varies depending on the entity or individual being notified. The Board will promptly implement the appropriate notification method below.

1. Notice to Individuals:
   a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available. If the Board knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to either the next of kin or personal representative of the individual.
   b. In the case in which there is insufficient or out-of-date contact information that precludes written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative
      i. In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.
      ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall be in the form of either a

conspicuous posting for a period of 90 days on the home page of the website of the Board, or conspicuous notice in major print or broadcast media in the Board's geographic areas where the individuals affected by the breach likely reside. Also, the notice shall include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's PHI may be included in the breach.

iii. In the event that the Board decides that notification requires urgency because of possible imminent misuse of unsecured PHI, the Board may provide information to individuals by telephone or other means, as appropriate, in addition to notice stated above.

2. Notice to Media

The Board shall provide notice to prominent media outlets serving the state and regional area if a breach of unsecured PHI involves more than 500 residents of a State or jurisdiction. The notice will be in the form of a press release.

3. Notice to Secretary of HHS

For breaches of unsecured PHI involving 500 or more individuals, the Board shall provide the notification to the Secretary of HHS as instructed at www.hhs.gov. at the same time notice is made to individuals.

For breaches of unsecured PHI involving less than 500 individuals, the Board shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, submit the annual log of breaches to the Secretary of HHS at www.hhs.gov.

E. Documentation of Breach Notice

The Board shall maintain the documentation related to the provision of notice to individuals, HHS, the media, if applicable, and any communication from law enforcement related to the delayed notification, if applicable, for at least six (6) years from the date notice was provided.

V. **Annual Review of Policy**

This Policy shall be reviewed and updated at least annually and on an as needed basis to incorporate any amendments to the HITECH Act related to providing notices of Breach of Unsecured PHI and any guidance issued by HHS relevant to this Policy.

VI. Maintenance of Breach Log

The Board shall maintain a process or record or log of all breaches of unsecured PHI regardless of the number of individuals affected. The Privacy Officer shall collect the following information for each breach:

A. A description of what happened, the date of the breach, the date of the discovery of the breach, and the number of individuals affected, if known;

B. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.);

C. A description of the action taken with regard to notification of individuals regarding the breach; and

D. Resolution steps taken to mitigate the breach and prevent future occurrences.

VII. Enforcement

This policy will be enforced by the Privacy Officer and/or Executive Team. Workforce members who violate this policy will be subject to disciplinary action up to and including termination from employment. Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the Privacy Officer. Where possible, every effort will be made to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment.

VIII. Definitions

Access. The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach. The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the protected health information. For purposes of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI.

Breach excludes. (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 was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

(2) Any inadvertent disclosure 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 was made would not reasonably have been able to retain such information.

Covered Entity. A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.

Disclosure. The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Individually Identifiable Health Information. Means that information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official. Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Protected Health Information (PHI). Individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information. PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is low probability of assigning meaning without the use of confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a devise or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
    a. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
    b. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in the following ways:
    a. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
    b. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce Members. Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.