BREACH NOTIFICATION – PROTECTED HEALTH INFORMATION POLICY

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacts the Health Insurance Portability and Accountability (HIPAA) Privacy and Security Rules. While HIPAA did not require notification when patient protected health information (PHI) was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH does require notification of certain breaches of unsecured PHI to the following: individuals, Department of Health and Human Services (HHS), and the media. The effective implementation for this provision is September 23, 2009.

DEFINITIONS

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

Breach: Means 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 PHI unless it can be demonstrated that there is a low probability that the PHI has been compromised. . A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2). 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 (CE) or Business Associate (BA) 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 CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE 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 CE or BA 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, and or a health care provider who transmits any health information in an electronic form.

Disclosure: Disclosure means 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: 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.

Organization: For the purposes of this policy, the term "organization" shall mean the covered entity to which the policy and breach notification apply.

Protected Health Information (PHI): Protected health information means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. Employment records held by a Covered Entity in its role as an employer are not PHI.

Unsecured Protected Health Information: 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 in the guidance issued under section 13402(h)(2) of Pub. L. 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 a low probability of assigning meaning without the use of a 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 device 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 Publications 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 Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

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

Policy:

1. Discovery of Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization's business associates). The organization 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 (business associate) of the organization (see attachment for examples of breach of unsecured protected heath information). Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response), conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been, accessed, acquired, used, or disclosed as a result of the breach. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.)

2. Breach Investigation: The organization shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager,

etc.). The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the organization will need to perform a risk assessment to determine if it can be demonstrated that there is a low probability that the PHI has been compromised. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

   (1) the nature and extent of the protected health information 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 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.

4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
B. 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 above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:
   A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   B. 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).
   C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
   E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

7. Methods of Notification: The method of notification will depend on the individuals/ entities to be notified. The following methods must be utilized accordingly:
   A. Notice to Individual(s): Notice shall be provided promptly and in the following form:
      1. 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 shall be provided in one or more mailings as information is available. If the organization knows that 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 the next of kin or person representative shall be carried out.
      2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A 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.

a. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

b. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization's website, or a conspicuous notice in a major print or broadcast media in the organization's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

3. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

B. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

C. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the **unsecured** PHI of more than 500 patients is accessed, acquired, used, or disclosed.

1. For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

2. For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

8. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the organization shall maintain a process to

record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach:

A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
B. A description of the types of unsecured protected health information 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 patients regarding the breach.
D. Resolution steps taken to mitigate the breach and prevent future occurrences.

9. Business Associate Responsibilities: The business associate (BA) of the organization that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the organization with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

10. Workforce Training: The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

11. Complaints: The organization must provide a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization's breach notification processes.

12. Sanctions: The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

13. Retaliation/Waiver: The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require

individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Examples of Breaches of Unsecured Protected Health Information

- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Misdirected e-mail of listing of drug seeking patients to an external group list.
- EOB (Explanation of Benefits) sent to wrong guarantor.

Breach Penalties

Penalties for Breach: Penalties for violations of HIPAA have been established under HITECH as indicated below. The penalties do not apply if the organization did not know (or by exercising reasonable diligence would not have known) of the violation or if the failure to comply was due to a reasonable cause and was corrected within thirty days. Penalties will be based on the organization's culpability for the HIPAA violation. The Secretary of HHS will base its penalty determination on the nature and extent of both the violation and the harm caused by the violation. The Secretary still will have the discretion to impose corrective action without a penalty in cases where the person did not know (and by exercising reasonable diligence would not have known) that such person committed a violation.

The maximum penalty is $50,000 per violation, with a cap of $1,500,000 for all violations of an identical requirement or prohibition during a calendar year.

The minimum civil monetary penalties are tiered based upon the entity's perceived culpability for the HIPAA violation, as follows:

Tier A – *If the offender did not know*

- $100 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $50,000.

Tier B – *Violation due to reasonable cause, not willful neglect*

- $1,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $50,000.

Tier C – *Violation due to willful neglect, but was corrected.*

- $10,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $50,000.

Tier D – *Violation due to willful neglect, but was NOT corrected.*

- $50,000 for each violation, total for all violations of an identical requirement during a calendar year cannot exceed $1,500,000.

Breach Notification Log

The organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. A record of the complete investigation of the potential breach as well as the risk assessment carried out to determine notification requirements should be created. The risk assessment and the record/incident report should be cross referenced so that should the Secretary of HHS require more information, it is easy to locate and provide.