

Procedure – Breach Assessment, Notification

Original Effective Date: 05/10/10	Revision Effective Date: 05/02/2012
-----------------------------------	-------------------------------------

These guidelines will assist with identifying the appropriate steps to take when a breach of protected health information (PHI) occurs.

Definitions under HITECH as it relates to the exchange of PHI.

Covered Entity (CE)-applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA. MS-HIN participants are defined as covered entities.

Business Associate (BA)-a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include without limitation claims processing, data analysis, utilization review, and billing. MS-HIN is defined as a Business Associate.

POTENTIAL BREACH ASSESSMENT

The MS-HIN participant's Privacy/Security Office designee will run the appropriate audit reports locally and will review the findings as soon as a potential breach has been detected. If needed, the designee may contact the MS-HIN Office for assistance with running reports. The MS-HIN participant should commence the breach investigation as soon as possible and no more than 7 days after being reported or suspected. MS-HIN participants will send the incident report and associated audit reports to the MS-HIN Director. If needed, MS-HIN legal counsel will review the findings before a final assessment is made.

STEPS: BOTH BUSINESS ASSOCIATES AND COVERED ENTITIES

- I. The designee should deactivate the participant's User ID at the time the incident is reported or suspected. The participants' User ID will remain inactive during the investigation period.
- II. Using the provided criteria, the designee will conduct an investigation and make a preliminary finding. If a breach is suspected, the participant will prepare an incident report using the criteria below and will notify the MS-HIN Office in writing.

The following questions will guide MS-HIN participants through an investigation of potential breach of PHI and ensure that MS-HIN meets the requisite HIPAA requirements.

Step 1 Was there a breach of unsecured PHI?

- Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule.
 - i) It is not a violation if the information was de-identified.

- ii) It is not a violation if information was disclosed for treatment, payment or operations.
- iii) Consult with MS-HIN legal counsel if you need advice concerning whether a breach has occurred.
- Was the PHI “unsecured”?
 - i) Was the information unusable, unreadable, and indecipherable through technology?
 - ii) Was the PHI secured through the use of a technology or methodology specified in guidance from HHS?
 - iii) Was the PHI a Limited Data Set that excludes zip codes and dates of birth?

Step 2 Did the use or disclosure compromise the security and privacy of PHI?

- Does the use or disclosure of PHI pose a significant risk of financial, reputation or other harm to the individual?
 - i) How many people were affected?
 - ii) What type of information was disclosed?
 - (1) Financial information
 - (2) Sensitive health information
 - iii) To whom was the PHI disclosed?
 - (1) A coworker
 - (2) A business associate
 - iv) Why did the disclosure occur?
 - (1) Unintentional
 - (2) Curiosity
 - (3) Intentional (i.e., theft, sales)
 - v) Who is the patient?
 - (1) Celebrity or Government Official
 - (2) Mentally ill patients
 - (3) Minors

Step 3 Was the breach unintentional, inadvertent, or otherwise excluded from the breach notification requirements?

- Was the breach unintentional or acquired by a staff member acting in good faith within the scope of his or her authority?
- Was the breach limited to that one staff member?
- Was the breach limited to two authorized persons?
- Was the disclosure to a person who would not reasonably have been able to mentally or physically retain the unsecured PHI?

III. BREACH CONFIRMATION

Based on a designee's role, the MS-HIN Board will require the following HIPAA guidelines be followed.

IV. BREACH CONFIRMATION – Business Associate Responsibilities Required by HIPAA

Following the discovery of a breach of unsecured PHI, a business associate shall notify the covered entity of the breach.

- i) Business associates must notify covered entities without unreasonable delay and in no case later than 60 days after discovery of the breach by the covered entity or its business associate (unless there is a law enforcement request for delay).
- ii) To the extent practicable, the business associate's notification to the covered entity must include: the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed during the breach. The business associate must provide the covered entity with any other available information that the covered entity is required to include in the notification to the individual.

V. BREACH CONFIRMATION - Covered Entity Responsibilities Required by HIPAA

A covered entity shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

A. Notification to Individuals

- i) All notifications to individuals must be made without unreasonable delay and in no case later than 60 days after discovery of the breach by the covered entity or its business associate (unless there is a law enforcement request for delay).
- ii) Notice to individuals must contain a description of what happened (including date of breach and discovery); the unsecured PHI involved; steps for individuals to protect themselves; a description of the covered entity's efforts to investigate, mitigate and prevent further breaches; and contact information for individuals to ask questions or learn additional information.
- iii) Written notice must be made by first-class mail to the individual at his/her last known address (or email if specified by the individual).
- iv) If there is insufficient or out-of-date contact information that precludes written notification to the individual, a covered entity must provide a "substitute form of notice."
 - If the breach involves fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.
 - If the breach involves 10 or more individuals with insufficient or out-of-date contact information, substitute notice must be:
 - By a conspicuous posting for 90 days on the home page of the covered

entity's website, or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside; and

- By a notice/posting including a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.
- v) If the covered entity deems urgency exists because of possible and imminent misuse of unsecured PHI, the covered entity may also provide information to individuals by telephone or other means, as appropriate.

B. Notification to the Media

- i) If the unsecured PHI of more than 500 residents of the State or jurisdiction are affected by the breach, the covered entity must provide notice to prominent media outlets serving the State or jurisdiction.
- ii) All notifications must be made without unreasonable delay and in no case later than 60 days of discovery of the breach by the covered entity or its business associate (unless there is a law enforcement request for delay).
- iii) Notice to media must contain a description of what happened (including date of breach and discovery); the unsecured PHI involved; steps for individuals to protect themselves; a description of the covered entity's efforts to investigate, mitigate and prevent further breaches; and contact information for individuals to ask questions or learn additional information.

C. Breaches Involving 500 or More Individuals

In addition to providing the required notifications to individuals and media (except as provided for law enforcement delay), the covered entity must provide notice in the manner specified on the HHS website.

D. Breaches Involving Fewer than 500 Individuals

In addition to providing the required notifications to individuals and/or media, covered entity must log the breach and disclose it to HHS in an annual report, no later than 60 days after the end of each calendar year.

E. Training

A covered entity must train all members of its workforce on the policies and procedures with respect to PHI and the applicable HHS breach notification.

F. Complaints to the Covered Entity

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures regarding by the breach notification.

G. Sanctions

A covered entity must have, apply, and document appropriate sanctions against members of its workforce who fail to comply with its privacy and breach notification policies and procedures.

A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for rights an individual exercises regarding the interim breach notification rule.

A covered entity may not require individuals to waive their rights as a condition of provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

H. Policies

With respect to PHI, covered entity must implement policies and procedures that are designed to comply with the interim breach notification rule and any applicable changes in federal law. A covered entity must change its policies and procedures as necessary and appropriate.

SAMPLE LETTER OF BREACH NOTIFICATION

[Date]

BY U.S. MAIL

[Name]

[Address Here]

[City, State Zip Code]

Dear [Name of Patient]:

We are writing to inform you about an information security situation that could potentially affect you and to share with you the steps we have taken to address it.

We discovered on [Insert the date the breach was discovered] that [Insert a brief, objective description of what happened, including the date of the breach.]

The personal health information involved includes [insert a description of the types of unsecured protected health information that were involved in the breach, such as full name, SSN, date of birth, gender, home address, account number, diagnosis, disability code, or other types of information. If appropriate, describe the information that was not involved, such as credit card numbers, bank account numbers, etc.]

We assure you that we are committed to safeguarding your sensitive personal information and have taken steps to fortify the protective measures that were already in place. As soon as this breach of information was discovered, [Name of Organization] [insert a description of what was done.] *[NOTE: Ensure that the description of how the incident was handled does not include any privileged information, i.e. we called our lawyers, had legal counsel order an investigation, produced a report, etc.]* Since the incident, we have [insert a description of what has been done to prevent a future breach].

[OPTIONAL] In addition, to help ensure that this information is not used inappropriately, we have made arrangements to offer you a free one-year membership to [insert name of credit monitoring company]. [Insert a brief description of how the monitoring works]. To take advantage of this offer, [describe the steps for the patient to initiate the monitoring].

While we are uncertain whether your personal information was actually obtained during the unauthorized access, we want to urge you to take actions to minimize your potential risk of identity theft. You may want to consider taking the following steps:

- Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report.

- Equifax: 1-800-525-6285; www.equifax.com
 - Experian: 1-888-397-3742; www.experian.com
 - TransUnion: 1-800-680-7289; www.transunion.com
- Order your credit reports. By establishing the fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
 - Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.
 - You can also place a “credit freeze” on your credit file so that no credit reports can be released without your approval. All bureaus charge a fee for this service.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. [Name of Organization] apologizes for the stress and inconvenience this situation has caused you. If you have any questions or require assistance regarding the loss of your personal information, please contact [insert name] at [insert phone number]. You may call Monday through Friday from 8:30 a.m. to 5:00 p.m. If you would prefer, you may contact us by email at [Insert email address] or by regular mail at [Insert postal address].

[OPTIONAL] We have also established a section on our Website with updated information and links to Websites that offer information on what to do if your personal information has been compromised.

Sincerely,