Chapter: 7	Section: 1	Subject: 2

CHAPTER: HIPAA		
SECTION: HIPAA Privacy and Security		
SUBJECT: Breach Notification		
Administrative Approval:	Date of Governing Board Action: February 16, 2010	Page 1 of 13

I. PURPOSE: To comply with requirements under HIPAA to establish procedures for a breach notification policy.

II. APPLICATION: West Michigan CMH as a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and their Business Associates.

III. REQUIRED BY: HIPPA Privacy Rule and Security Rule 45 CFR and Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) enacted on February 17, 2009.

IV. DEFINITIONS: Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under Subpart E of 45 CFR Part 164 which compromises the security or privacy of the protected health information.

V. POLICY: It is the policy of West Michigan Community Mental Health to provide for notification in the case of breaches of unsecured protected health information.

VI. PROCEDURES:

1. Breach Notification Team.

   West Michigan CMH has established a Breach Notification Team, which consists of the following members:

   - Regulations/Privacy Officer
   - Security Officer
   - Records Supervisor (custodian of the records at issue or otherwise considered responsible for the records). This may also include a representative of a business associate that maintains protected health information on behalf of WMCMH.
   - Members of the WMCMH Corporate Compliance Committee including ad hoc members, as necessary.
   - General legal counsel/outside legal counsel, as necessary.

   In the event of a potential breach of protected health information, WMCMH will investigate the incident consistent with its regulatory management procedures. One or more members of the Breach Notification Team will participate in such

investigation and report relevant facts to applicable team members for purposes of determining whether notification will be required.

In determining whether notification is required, the Breach Notification Team may consult with any additional employees, agents, contractors or consultants reasonably necessary to determine whether WMCMH has a duty to notify individuals about a breach.

2. Determine whether a breach has occurred.

When WMCMH learns of a possible breach, the Breach Notification Team must determine whether there has been an impermissible use or disclosure of unsecured protected health information under HIPAA's Privacy Rule. This includes situations in which a contractor/business associate notifies WMCMH that an impermissible use or disclosure has or may have occurred. The following are examples of the types of situations that may need evaluation:

- WMCMH learns that an unauthorized individual has gained access to WMCMH's electronic information system.
- WMCMH learns that an authorized individual may have accessed protected health information for an improper purpose.
- WMCMH learns that information intended for an authorized individual was misdirected (for example, by e-mail or fax transmission).
- WMCMH learns that a business associate has suffered a potential data breach.
- WMCMH hears from individuals who are the subject of the WMCMH's protected health information that they have been the victims of identity theft or other identity fraud crime.

If a situation requires evaluation, the Breach Notification Team or designee should gather details about the incident, including the following:

- The specific data that is involved in the incident.
- Whether the access, use or disclosure is consistent with WMCMH's HIPAA policies and procedures.
- The manner in which the information was accessed, used or disclosed.
- The date the incident was discovered.
- The date(s) the incident occurred.

- The number of individuals whose information was involved.
- The states in which the individuals reside.

Note: while this policy addresses breach notification requirements under HIPAA, the Breach Notification Team may need to consult with legal counsel to determine if WMCMH has any obligations under Michigan notification laws—whether or not notification is required under HIPAA.

Note: in the event of a breach, WMCMH will also need to evaluate the effectiveness of its privacy and security practices and determine whether changes need to take place, consistent with WMCMH's HIPAA evaluation procedures.

If the facts indicate that the access, use, or disclosure was not permitted under HIPAA, the Breach Notification Team will need to determine whether the incident falls into one of the exceptions to the HIPAA breach notification requirements. WMCMH may not have a duty to notify if (A) The information is considered "secured"; (B) The incident is not considered a "breach"; or (C) There is a low probability that the PHI has been compromised based on a risk assessment.

A. Determine whether the information is deemed "secured" under HIPAA.

The first step is to determine whether the information was properly secured under HIPAA. Whether the information is properly secured will depend on the nature of the information and how well it is protected.

- If the information is electronic, the data is considered secured if *both* of the following are true:

    1. The data has been properly encrypted consistent with guidance issued by the Department of Health & Human Services. This guidance may change from time to time, but as of September 2009, HHS guidance called for the following:

        - For data at rest (including data that resides in databases, file systems, flash drives, memory and other structured storage methods), the encryption process must be consistent with National Institute of Standards & Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices.*

- For data in motion (which includes data moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange), the encryption process must comply, as appropriate, with one of the following:

  - National Institute of Standards & Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*;

  - National Institute of Standards & Technology Special Publication 800-77, *Guide to IPsec VPNs;*

  - National Institute of Standards & Technology Special Publication 800-113, *Guide to SSL VPNs*; or

  - Other encryption processes that are Federal Information Processing Standards 140-2 validated.

2. The individual/entity with improper access to the information does not have access to the confidential decryption process or key.

- Data that has been destroyed may also be considered secured if one of the following is true:

  1. The information was stored on paper, film or other hard copy media, and the media has been shredded or destroyed in such a way that the protected health information cannot be reconstructed. (Note that redaction is **not** an effective form of destruction.)

  2. The information is in electronic form and has been cleared, purged or destroyed consistent with National Institute of Standards & Technology Special Publication 800-88, *Guidelines for Media Sanitization*, so that the protected health information cannot be retrieved.

If the information meets one of the tests above for being secured, the incident will not be considered a breach and notification will not be necessary.

If the Breach Notification Team concludes that the information is secured, it must document the facts leading to this conclusion. The documentation must be retained for a period of at least six years from the date the Team concludes its evaluation of the incident.

B. Determine whether the incident falls within an unintentional acquisition, inadvertent or disclosure exception.

If the information is not considered secured, the incident may still not be considered a breach if the incident falls within one of the following exceptions:

1. Unintentional acquisition, access or use of protected health information. In order for this exception to apply, all of the following have to be true:

    a. the unauthorized acquisition, access or use of protected health information must have been unintentional;

    b. the individual who acquired, accessed or used the protected health information must be one of the following:

    - A member of WMCMH's workforce
    - A member of a business associate's workforce
    - A person acting under the authority of WMCMH or WMCMH's business associate

    c. The individual who acquired, accessed or used the protected health information did so in good faith.

    d. The acquisition, access or use did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

2. Inadvertent internal disclosure of protected health information. This exception applies if all of the following are true:

a. The disclosure is made *by* an individual who is authorized to access protected health information

b. The disclosure is made *to* an individual who is authorized to access protected health information.

c. Both individuals work for the same organization, which may be one of the following:

- WMCMH
- WMCMH's business associate
- An organized health care arrangement in which WMCMH participates.

d. The disclosure did not result in any further use or disclosure that is not permitted under the HIPAA privacy rules.

3. Where the information would not be retained. This exception applies if all of the following are true:

a. The disclosure is made to an unauthorized individual.

b. WMCMH or its business associate has a good-faith belief that the unauthorized individual would not reasonably have been able to retain the information.

If the Breach Notification Team concludes that the incident meets one of the exception tests above, the incident will not be considered a breach and notification will not be necessary. The Team must document its analysis leading to this conclusion. The documentation must be retained for a period of at least six years from the date the Team concludes its evaluation of the incident.

C. Demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.

The Breach Notification Team must demonstrate that there is a low probability that the unauthorized acquisition, access, use or disclosure of PHI has been compromised based on a risk assessment of at least the following factors:

- **(i) Whether the PHI was actually acquired or viewed**
  - Are there past dealings with the receiver or other factors that would indicate that the receiver can be trusted not to use or further disclose the information?
  - Was the information returned before being accessed for an improper purpose?

- **(ii) The unauthorized person who used the PHI or to whom the disclosure was made**
  - Who impermissibly acquired, accessed or used the information or whom was the information impermissibly disclosed?
  - Was the receiver also a HIPAA covered entity with a legal duty not to misuse the information?
  - Does the receiver have a contractual relationship with WMCMH that prohibits it from misusing the information?
  - Are there other facts and circumstances that would indicate that the receiver of the information is unlikely to misuse the information?

- **(iii) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification**
  - How much detailed information was included in the data?
  - Did it include social security numbers, driver's license numbers, bank account/credit card numbers, insurance numbers, or other sensitive information that could be used for identity theft or identity fraud crimes?
  - Did it include information about medical treatment, diagnoses, diseases, or similar details about an individual's health?

- **(iv) The extent to which the risk to the PHI has been mitigated**
  - Were immediate steps taken to mitigate an impermissible use or disclosure, such as by obtaining the receiver's satisfactory assurances that the information will not be further used or disclosed or will be destroyed?
  - The Breach Notification Team should consider these and other pertinent facts to determine whether the security or privacy of individuals PHI is compromised.

- If the Breach Notification Team demonstrates that there is a low probability that the PHI has been compromised then notification is not required. The Team must document its risk assessment leading to this conclusion and retain this documentation for at least six years from the date the Team concludes its evaluation of the incident.

3. Special considerations for breaches involving Business Associates (or for business associates, subcontractors)

   Under HIPAA, a business associate who maintains protected health information on behalf of WMCMH has a duty to notify WMCMH of the breach within 60 days, but it is WMCMH's duty to provide notification to the individuals impacted by the breach. Moreover, in certain circumstances, WMCMH may be charged with the business associate's knowledge of the breach, so that the deadline for providing notice will be based upon when the business associate knew or should have known about the breach.

   In order to reduce the risk to WMCMH of a HIPAA violation, WMCMH will seek to include in its business associate agreements a provision that requires the business associate to notify WMCMH of a potential breach within 3 business days of discovery and to provide information about the individuals involved in the potential breach within 30 days of discovery. When appropriate, and after reaching consensus with business associate, WMCMH may also include a provision in the business associate agreement allocating responsibility for notification between WMCMH and business associate. When a business associate reports a potential breach to WMCMH, the Breach Notification Team will work with the business associate to determine whether the incident requires notification.

4. Notification

   If the Breach Notification Team determines that WMCMH must provide notification of the incident, the Team designee will prepare appropriate notification as required below.

   A. Notice to Individuals

   Under HIPAA, WMCMH must provide notice to affected individuals without unreasonable delay, but no later than 60 days after the date WMCMH discovers the breach or should have discovered the breach if it had exercised

appropriate diligence. In order to reduce the risk of exceeding the deadline, WMCMH will seek to provide notice as soon as reasonably possible once it has discovered the breach.

The HIPAA breach notification regulations require that the following information be included in the notification:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
- A description of the types of unsecured protected health information that were involved in the breach.
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what WMCMH is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an e-mail address, Website, or postal address.

All notifications must be written in plain language.

Notice may be provided by e-mail to individuals who have agreed in advance to receive electronic notice and per WMCMH policy. Otherwise, notice must be sent via first class mail. If WMCMH knows that an individual is deceased and has the address of the deceased's next of kin or personal representative, WMCMH may send the written notification to either next of kin or the personal representative.

Under HIPAA, WMCMH has no more than 60 days after discovery of the disclosure to notify individuals. The date of discovery is measured as follows:

- First day the breach is known to a member of the WMCMH's workforce or agents;

- Workforce member includes any employee, partner, volunteer, trainee, agent, etc.

- First day a member of the WMCMH workforce or its agents **would have known** of the breach by exercising reasonable diligence; or

- First day that WMCMH is notified of a breach by any of its independent contractors (unless the independent contractor is deemed to be an agent).

Note: Michigan security breach notification laws may also apply and may mandate a shorter time frame for notification.

If WMCMH does not have sufficient contact information for some or all of the affected individuals (or if the contact information is outdated) then WMCMH must provide substitute notice for such individuals in the following manner:

- If fewer than 10 individuals are affected, substitute notice can be provided to these individuals via telephone or other written notice that is reasonably calculated to reach the individuals.

- If more than 10 individuals are affected, HIPAA requires the following:

  - a conspicuous posting for a period of 90 days on WMCMH's home page, if applicable **or** a conspicuous notice in a major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside; and

  - A toll-free phone number active for 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

- The content of the substitute notice must include all of the elements required for the standard notice described above.

- Substitute notice is not required in situations where an individual is deceased and WMCMH does not have sufficient contact information for the deceased individual's next of kin or personal representative.

If WMCMH believes that there is the possibility of imminent misuse of unsecured protected health information WMCMH may also provide expedited notice by telephone or other means. This notice is in addition to, and not in lieu of, direct written notice.

WMCMH must retain copies of all notifications for at least six years from the date the notifications were provided. For substitute notifications, retain copies for at least six years from the date the notification was last posted on the website, if applicable or the date the notification last ran in print or broadcast media.

B. Notice to the Media

If the Breach Notification Team determines that notification is required to more than 500 residents of Michigan, WMCMH must provide notice in the form of a press release to prominent media outlets serving the state. The press release must include the same information required in the written notice provided to individuals. The Breach Notification Team may coordinate such notice with WMCMH's public relations resources or other public relations consultants, as appropriate.

Note: Michigan security breach notification laws should also be consulted to determine whether there are additional notification obligations to the media, state agencies, or national credit bureaus.

WMCMH must retain copies of all press releases provided to prominent media outlets for at least six years from the date the notifications were provided.

C. To the Department of Health & Human Services

If the Breach Notification Team determines that WMCMH or its business associate must provide notification to individuals under HPAA, then WMCMH will also have to provide notification to the Department of Health & Human Services. The timing of the notification will depend on the number of individuals affected by the incident:

- If the breach involves more than 500 individuals (regardless of whether they reside in the same state or in multiple states), WMCMH will notify

the Department of Health & Human Services without unreasonable delay, but no later than 60 days after discovery. This notification is to be submitted to the Department of Health & Human Services contemporaneously with the written notifications sent to individuals and in the manner specified on the Department's Web site.

- If the breach involves fewer than 500 individuals:
    - The Privacy Officer must maintain a log or other documentation of notifications involving fewer than 500 individuals. The information to be recorded in the log will be set forth on the Department of Health & Human Services' Web site.
    - The Privacy Officer will submit the log to the Department of Health & Human Services for each calendar year by February 28 of the following year, in the manner specified on the Department's Web site.

Notifications to the Department of Health & Human Services, including the annual log of notifications, must be maintained for at least six years from the date submitted to the Department.