Holyoke Medical Center, Inc.

CHAPTER: Management of Information	**POLICY # A10-128**
SUBJECT: Breach Notification Regulations	**Page 1 of 4**
Date Initiated: 12/1/09	**Date Reviewed/Revised: 10/2010**
Distribution: ALL HOLDERS OF ADMINISTRATIVE POLICY MANUAL	

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). This new regulation significantly impacts the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. HITECH requires mandatory notification for breach of protected health information (PHI).

DEFINITION:
Breach – The unauthorized acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. (Disclosure poses a significant risk of financial, reputational or other harm to the individual).

POLICY:
Holyoke Medical Center will follow the Breach Notification Regulations of the above law.

PROCEDURE:

DISCOVERY OF A BREACH:
The breach is considered discovered on the first day on which it is known to the organization, or by exercising reasonable diligence would have been known to the organization.

The person who discovers the breach must immediately fill out a Breach of PHI Reporting Form **(Attachment A),** located on the Hospital's Intranet which will be automatically e-mailed to the Privacy Officer and Compliance Officer.

Covered entities (CE) and Business Associates (BA) have a maximum of sixty (60) days to report the breach to the individual but the notification should be done without reasonable delay.

BREACH INVESTIGATION:
Following the discovery of a breach, the hospital will begin an investigation (lead by the Privacy Officer and Compliance Officer), conduct a risk assessment, and depending on the results of the assessment, start the process of notifying the patient whose PHI was breached, and other appropriate outside agencies if required.

ALL DOCUMENTATION MUST BE RETAINED FOR SIX (6) YEARS.

RISK ASSESSMENT:
The risk assessment must be fact specific and well documented.

1. Who impermissibly used or to whom the information was impermissibly disclosed
2. The type and amount of PHI involved
3. The potential for significant risk of financial, reputational or other harm.

If the risk assessment determines there was significant risk of harm to the individual as a result of the breach, then the secretary of HHS and possibly the media will be notified depending on the number of individuals whose PHI was breached.

LOG BREACH:
A log of all potential breaches must be kept along with the complete documentation of the investigation, including the reason why it is or is not considered a breach.

NOTIFICATION:
Must be made to the patient without unreasonable delay and no later than sixty (60) calendar days after the day the breach was discovered.
The facility must be able to show that all notices were made as required, including evidence demonstrating the necessity of any delay.

LAW ENFORCEMENT DELAY:
If a law enforcement official states to a CE or BA that a required notification, notice or posting would impede a criminal investigation or cause damage to national security, then the CE or BA will:

1. When the statement is in writing and specifies the time for which a delay is required, delay notification, notice, or posting for the time period specified by the official; or
2. When the statement is oral, document the statement, including the identity of the official making the statement and delay the notification, notice, or posting temporarily and not longer than 30 days from the date of the oral statement, unless a written statement is received within the required time period.

CONTENT OF THE NOTIFICATION:
The notification to the patient must be written in plain language and contain the following:

- 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 PHI that were involved in the breach.
- Any steps individuals should take to protect themselves from potential harm resulting from the breach.

- A brief description of what the CE involved 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, Web site, or postal address.

METHODS OF NOTIFICATION:

1. To the Individual –

Written Notice:

- Notice must be by first-class mail to the last known address of the individual or their representative, or
- The notice can be sent by electronic notice if that has been the agreed upon form of notice between the entity and the individual and this agreement has not been withdrawn.
- The notification may be provided in one or more mailings as more information is made available.
- If the individual is deceased then the notice following the same rules must be sent to the next of kin or the personal representative as specified in the Privacy Rule.

Substitute Notice:

- If the written notice cannot be received due to insufficient or out-of-date contact information, a substitute form of notice must go out. If the individual is deceased and the next of kin or personal representative cannot be contacted, no additional steps must be taken with a substitute notice.
- The substitution notice varies depending on the number of individuals impacted by the breach:
  - If less than ten (10) individuals are involved the substitute notice can be by phone or other means.
  - If ten (10) or more individuals are involved, the substitute notice will:
    1. Be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the web site of the CE involved OR a conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside, **AND**
    2. Include a toll-free number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHR may be included in the breach.

**HHS has provided even more detail in the Preamble including how a substitute notice should be posted on the covered entities web site and what constitutes choosing media in a geographic area.

2. To the Media -
   - For a breach involving more than 500 residents of a State or jurisdiction, a CE must notify prominent media outlets serving the State or jurisdiction. (If the number of individuals is greater than 500 but multiple states are involved and no one state has 500, it is possible that no notification is necessary) Notification must be done without unreasonable delay and no later than sixty (60) calendar days after the discovery of the breach except for law enforcement delays.

3. To the Secretary of HHS -
   - Breaches involving 500 or more individuals require notice to the secretary at the same time notice is sent to the individual. (The manner of the notice is specified on the HHS web site)
   - Breaches involving less than 500 individuals require documentation in a log which will be sent to the secretary no later than sixty (60) days after the end of each calendar year.

BUSINESS ASSOCIATES:
Business Associates must notify the CE of any breach. Then the above procedure must be followed.

WORKFORCE TRAINING:
A CE must provide training that meets the following requirements:
- Each member of the CE's workforce must be trained no later than February 22, 2010 and then annually.
- Each new member of the workforce must be trained within a reasonable period of time after the person joins the CE's workforce.
- Each time the policy changes members of the workforce must be re-trained.
- A CE must document that the training has been provided.

BREACH OF PHI REPORTING FORM
HOLYOKE MEDICAL CENTER

Complete this form as soon as potential breach is discovered, then hand deliver this form to the Privacy Officer immediately (Compliance Officer if Privacy Officer is unavailable).

1. Date of breach (if known) _____

2. Date of discovery of breach _____

3. How was breach discovered: _____

4. Patient Name(s): _____

5. Patient Medical Record Number: _____

6. Brief description of the breach: _____

_____

_____

7. Number of patients involved: _____

8. Person reporting the breach/Department/Extension:

_____