Date: December 15, 2009
To: UW-Madison HIPAA Contacts
From: Rebecca Hutton, UW-Madison HIPAA Privacy Officer
Subject: Recent Changes in HIPAA Regarding Information Breaches (effective 09/17/09; enforced 02/10)

I. Covered entities are required to notify patients and others of “breaches” of “unsecured protected health information” that pose a “significant risk of financial, reputational, or other harm” to the individual.

A. “Secured” means not just protected, but “unusable, unreadable, or indecipherable to unauthorized individuals”
   1. Electronic PHI is considered unsecured unless it is encrypted according to certain specifications.
   2. PHI recorded on paper or other media is by definition never secured until confidentially destroyed.

B. “Breach”: the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. Exceptions:
   1. The unauthorized acquisition, access, or use of PHI is unintentional and made by an employee or individual acting under the authority of a covered entity if made in good faith and within the course and scope of employment (or other professional relationship) and such information is not further acquired, accessed, used or disclosed; or
   2. Where an inadvertent disclosure occurs by an individual who is authorized to access PHI at a facility operated by a covered entity to another similarly situated individual at the same facility, as long as the PHI is not further acquired, access used or disclosed without authorization.

C. “Significant risk of financial, reputational, or other harm”: Is not defined in the regulations, but guidance indicates that covered entities must do a case-by-case fact-specific risk of harm assessment whenever there is a breach of unsecured PHI, to determine if there is a significant risk of harm.

D. Notification Requirements:
   1. Must notify individual in writing. Notice must include:
      a. brief description of what happened, including the date of the breach and the date of the discovery of the breach,
      b. description of types of unsecured PHI involved,
      c. steps individuals should take to protect themselves,
      d. brief description of what covered entity is doing to investigate, mitigate and prevent future similar breaches, and
e. contact procedures for individuals to ask questions.

2. If there is insufficient or out-of-date contact information for 10 or more affected individuals, covered entity must place a conspicuous posting on its home page or conspicuous notice in major print or broadcast media along with a toll free number for additional information.

3. If more than 500 residents of a state affected, the covered entity must provide notice to prominent media outlets and notice to Secretary of US DHHA (annual notice to Secretary is required for all other breaches)

4. Secretary will post on US HHS website a listing of each covered entity with breaches involving 500 or more individuals.

E. What You Should Do

1. Report any potential breaches (including unauthorized uses) of PHI to the UW-Madison HIPAA Privacy Officer immediately so that determination can be made if notification required.
2. Encourage IT staff and others to make known to you issues about information privacy and security that are not promptly addressed. Act on concerns regarding information privacy and security reported by IT staff. Promote a culture of identifying and promptly correcting such concerns. Make sure your unit follows best practices. E.g.:
   a. Do not use personal email to transmit or store PHI.
   b. Do not share passwords.
   c. Do not forward UW, UWMF, or UW Health email to a non-UW email address.
   d. Encrypt all PHI on portable devices.
   e. Remove access to PHI immediately when employees are terminated or resign; promptly notify UWHC and UWMF of termination/resignation.
   f. Consult with IT staff whenever changing procedures for storing or transmitting PHI or when new projects/studies are implemented that involve storing or transmitting electronic PHI.

II. HITECH also increases penalties

A. If violation is the result of “willful neglect”, HHS may assess a penalty in the amount of $50,000 per violation up to $1.5 million per calendar year, even if corrected within 30 days of discovery. If not corrected within 30 days of discovery, no ceiling on total amount per year.

B. Harmed individuals may share in civil monetary penalties

C. State attorney generals able to bring enforcement actions (may bring civil action on behalf of harmed state residents)

Questions? Contact UW-Madison HIPAA Privacy Officer: Rebecca Hutton  
( rhutton@vc.wisc.edu or 263-7400)