

NEW HIPAA BREACH NOTIFICATION PROVISIONS GO INTO EFFECT WEDNESDAY!

You may remember in our ARRA HIPAA webinar conducted in June, we noted that the probable September effective date for the breach notification provisions was really just around the corner. Guess what: we're here.

The American Recovery and Reinvestment Act of 2009 ("ARRA") made several changes to the HIPAA privacy rules. The law imposed an explicit requirement on covered entities and their business associates to notify individuals when their covered data has been compromised. As we reported previously, this section of the act takes effect for breaches discovered 30 days after HHS published interim final regulations; HHS published those interim final regulations on August 24, 2009.

HHS's interim final regulations lay out the specific steps that HIPAA-covered entities and their business associates must take in determining whether there has been a breach and then in addressing any breach. Importantly, HHS stated that, while the breach notification requirements and procedures become effective on September 23, *it will not impose sanctions for failure to provide the required notifications for breaches discovered through February 22, 2010*. Instead, during this initial period, it will work with covered entities to achieve compliance through technical assistance and voluntary corrective action.

What the Interim Regulations Say In A Nutshell

Let's back up a step first. As required by ARRA, on April 17, 2009, HHS issued guidance regarding the technologies and methodologies that render PHI secured. That guidance created a safe harbor so that covered entities and business associates would not be required to provide the breach notifications required by ARRA for PHI meeting these standards. The guidance specified encryption and destruction as the only technologies and methodologies that rendered PHI secured. Remember that the breach notification requirements apply only if all of the following are present:

- There is a "breach." The interim final regulations define "breach" to mean (subject to exceptions) the unauthorized acquisition, access, use, or disclosure of PHI.
- The PHI is "unsecured." The interim final regulations define "unsecured protected health information" to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.
- The breach "compromises the security of the PHI." Under the interim final regulations, this occurs when there is a significant risk of financial, reputational, or other harm to the individual whose PHI has been compromised.

Also keep in mind that failure to render PHI “unusable, unreadable, or indecipherable to unauthorized individuals” – i.e., dealing with PHI that is “unsecured” under the regulations – is not a violation of HIPAA. It simply takes away a safety net that might make a breach notification unnecessary.

What’s a Breach?

The interim final regulations envision that covered entities and business associates will look at the following in determining whether a breach of unsecured PHI has occurred:

(1) Whether the use or disclosure of PHI violates the HIPAA Privacy Rule: for an acquisition, access, use, or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule.

(2) Whether there is a use or disclosure that compromises the security and privacy of PHI: HHS clarified that a use or disclosure that “compromises the security and privacy of PHI” means a use or disclosure that “poses a significant risk of financial, reputational, or other harm to the individual.” This is a definite improvement over our previous understanding of breach notification requirements; commenters had suggested that HHS add a “harm threshold” so that insignificant and unthreatening unauthorized uses or disclosures would not be considered a breach. HHS listened and established that, in order to determine whether a breach has occurred, covered entities and business associates will need to conduct a risk assessment to determine whether the potential breach presents a significant risk of harm to individuals as a result of an impermissible use or disclosure of PHI.

(3) Whether any Exceptions to the Breach Definition Apply: The interim final regulations discuss a number of exceptions to the definition of breach. The following three situations are specifically excluded from the definition of “breach” under the Act:

- The unintentional acquisition, access, or use of PHI by any workforce member or person acting under the authority of a covered entity or business associate, 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 by the Privacy Rule.
- The inadvertent disclosure of PHI by an individual otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another person at the same covered entity or business associate, or at a organized health care arrangement in which the covered entity 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.

- An unauthorized disclosure where a covered entity or business associate has a good faith belief that an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

What is Secured PHI?

PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if one or more of the following methods are used:

(1) *Encryption.* Electronic PHI is only secured where it has been encrypted. The HIPAA Security Rule specifies encryption to mean the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. The interim final regulations identify the various encryption processes which are judged to meet this standard. To avoid a breach of the confidential process or key, decryption tools should be kept on a separate device or at a location separate from the data they are used to encrypt or decrypt.

(2) *Destruction.* Hard copy PHI, such as paper or film media, is only secured where it has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. HHS noted specifically that redaction is insufficient to secure PHI; however, HHS also noted that de-identified information (remember, that's a term of art with very specific requirements) would no longer be PHI and therefore would not be subject to breach notification.

Notification Requirements

The breach notifications required by ARRA and the interim final regulations are triggered by the "discovery" of the breach of unsecured PHI. A breach is treated as "discovered" by a covered entity as of the first day the breach is known, or reasonably should have been known, to the covered entity. Given that knowledge of a breach may be imputed, a covered entity should implement reasonable breach discovery procedures and training for its workforce dealing with PHI.

Notification to Individuals: A covered entity must send the required notification to each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the breach, without unreasonable delay and in no case later than 60 calendar days after the date the breach was first discovered by the covered entity.

For covered entities that do not have sufficient contact information for some or all of the affected individuals, the interim final regulations require that substitute notice be provided as soon as reasonably possible. If a covered entity has insufficient contact information for 10 or more individuals, then substitute notice must be provided via a posting for a period of 90 days on the home page of its

website or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. In such instances, the covered entity is also required to have an active toll-free number for 90 days so that an individual can find out whether his or her unsecured PHI may be included in the breach.

Notification to Media: If a covered entity discovers a breach affecting more than 500 residents of a state or jurisdiction, it must provide notice to prominent media outlets serving that state or jurisdiction without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered by the covered entity.

Notification to HHS: If more than 500 individuals are involved in the breach, regardless of whether the breach involved more than 500 residents of a particular state or jurisdiction, then the covered entity must notify HHS concurrently with the individual notifications. For breaches involving fewer than 500 individuals, the covered entity must maintain an internal log or other documentation of such breaches and annually submit such log to HHS. For calendar year 2009, the covered entity is only required to submit the log for breaches occurring on or after September 23, 2009.

Notification by a Business Associate: Following the discovery of a breach of unsecured PHI, a business associate is required to notify the covered entity of the breach so that the covered entity can, in turn, notify the affected individuals. To the extent possible, the business associate should identify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached. Such notice should be given without unreasonable delay and no later than 60 days following discovery of a breach.

This update was prepared by Donna Eich Brooks, an attorney with the law firm of Lehr, Middlebrooks, & Vreeland. Donna can be reached for questions at dbrooks@lehrmiddlebrooks.com or at (205) 226-7120.

Lehr Middlebrooks & Vreeland, P.C.
P.O. Box 11945
Birmingham, AL 35202-1945
(205) 326-3002

The Alabama State Bar Requires The Following Disclosure:
"No Representation Is Made That The Quality Of The Legal Services To Be Performed
Is Greater Than The Quality Of Legal Services Performed By Other Lawyers."