KEY POINTS ON INTERIM BREACH FINAL RULE

UNSECURED Protected Health Information:

- Protected health information that is not secured through the use of technology or methodology.
- Must render data unusable, unreadable, or indecipherable.
- Allowed to use any methods that will reasonably and appropriately protect information.
- Must CONSIDER encryption but not necessarily non-compliant if not using it.
- If you chose not to encrypt according to HHS standards, and you rely on other protections, you would still have to follow notification principles in case of Breach.
- Data in motion, data in rest, data in use
- Encryption keys should be kept on a separate device from the data they encrypt.
- Considered unusable, unreadable is it:
  - Meets the encryption standards laid out by NIST.
  - The media on which PHI is stored has been destroyed in an appropriate way.

Breach and Breach Notification:

- Breach: the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
- De-identified information is not protected health information
- Employment records held by the covered entity do not count as protected health information although other notification laws may apply.
- First step is: Does it violate the privacy rule?
- A use or disclosure of protected health information that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule, and therefore would not qualify as a potential breach.
- Second step: Does it compromise the security or privacy of the protected health information.
- Must pose a significant risk of financial, reputational, or other harm to the individual.
- Must perform a risk assessment to evaluate the risk of harm.
- A limited data set counts as protected health information for purposes of breach unless the information also does not include zip codes or dates of birth. Must still perform a risk assessment.
• Covered entities bear the burden to prove that something did not constitute a breach. Must document risk assessment.

• Exceptions to breach:
  o Unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate.
  o Inadvertent disclosure of protected health information from one person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate.
  o Disclosures where the unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

Notice requirements:

• A covered entity shall provide notice to individuals when a breach occurs
• Treated as discovered the first day the breach is known, or by reasonable diligence should have been known.
• By any person, employee or agent, of the covered entity.
• Covered entities are liable for notifying individuals when a breach occurred and they “should” have known, so must implement a system of discovery.
• Send the notice with no unreasonable delay and no later than 60 days after discovery by the covered entity.
• Notification must include:
  o Brief description of what happened
  o Date of discovery and date of breach
  o Description of the types of PHI involved
  o Any steps an individual should take to mitigate harm
  o A brief description of what the covered entity is doing to mitigate
  o Contact procedures for additional information
• Must make notifications in clear easy to understand language, and may need to use braille or large print depending on audience.
• Must provide notice in written form, to the last known address. May be electronic if individuals previously agreed to it.
• If an individual is a minor or an individual lacking mental capacity, notice to the parent/guardian is sufficient.
• If patient is deceased notice must be sent to last known address of next of kin. Only required to do this if CE knows that individual is deceased and knows the address of the next of kin. If no known address, must provide substitute notice.
• Substitute notice must have all the same information as normal notice, must be reasonably calculated to reach the individuals.
• If under 10 individuals, substitute notice can be done through phone or email. Or post it on your webpage.
• 10 or more individuals, must either have a conspicuous notice on the webpage for 90 days, or in the media. Set up a toll free number for individuals to call.
• In urgent situations you may use ADDITIONAL notice such as telephone and email as well as written.
• More than 500 people at once: must provide notice to major media sources. Intended to supplement but not substitute individual notice.
• The 500 individuals must all be within one state for the notice provisions to kick in. For instance, if 200 were from one state, 200 from another, and 200 from a third, then it would not apply. Notification to the secretary would still apply.
• If a BA breaches, CE must provide the notice, but is a BA has 800 individuals breached, but only 450 are from one particular covered entity, then there is no media or secretary notice required.
• For breaches of 500 or more notice must be sent to the Secretary immediately. Immediately being interpreted as when notice is provided to the individuals.
• This notification is triggered with the total number of people, even if the 500 people are split between states. This means that you wouldn’t have to notify the media immediately, but you would have to notify the secretary.
• Must submit the log of breaches to HHS no later than 60 days from the end of the calendar year.
• Must maintain the log and documents for 6 years, pursuant to HIPAA.

Notification from business associates:
• Business associates must notify the covered entity when a suspected breach has occurred.
• The covered entity is the one that must notify the individuals.
• Same rules apply for when the breach is “discovered”, rules of agency, as well as rules of “reasonable diligence”.
• If the business associate is acting as an agent of the covered entity, then the 60 days for notification begins when the BA discovered the breach!!!
• If the BA is acting as a contractor of the covered entity, the 60 day notification begins when the BA informs the CE of the breach.
• Because we have the burden of proof to show notifications were made, or that a risk assessment was done and notifications were not necessary, we MUST document these items.
• HHS will start imposing sanctions for failure to notify as of February 22, 2010.