United Actuarial Services, Inc.
Actuaries and Consultants

2009-50

August 24, 2009

SPECIAL BULLETIN

Interim Final HIPAA Privacy Rule Breach Notification Regulation Published

The Department of Health and Human Services (HHS) issued an *Interim Final Rule* concerning the new requirement for notification to individuals and others of breaches of unsecured (unencrypted) protected health information (PHI). See *Research Memo 2009-47* for details on this new statutory requirement under the *American Recovery and Reinvestment Act of 2009 (ARRA*).

The *Interim Final Rule* was published in the *Federal Register* (74 FR 42740) and is available at *http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf* or by "*clicking here*." The *Preamble* contains a section-by-section analysis of the *Interim Final Rule* at pages 5 through 19 of the PDF version, with the new regulations at pages 29-32. A copy of just the main new breach notification regulation with a table of contents added is available by "*clicking here*."

This *Interim Final Rule* is **effective September 23, 2009** and essentially applies to all "covered entities" under the *HIPAA Privacy Rule* and also to the *Business Associates* of such covered entities. Although the law applies to all "covered entities" (health plans, health care clearinghouses and health care providers), for simplicity's sake we will generally just refer to "Health Plans."

In the *Preamble*, HHS stated it would use its enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before February 22, 2010. During this initial time period, after the rule has taken effect but before HHS begins imposing sanctions, HHS expects Health Plans to comply with this new breach notification rule. HHS will work with Health Plans, through technical assistance and voluntary corrective action, to achieve compliance.

The general principle under the *Interim Final Rule* is that following the discovery of a breach of unsecured PHI, a Health Plan should notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as a result of such breach.

Prepared by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

In a bit of good news, the *Interim Final Rule* limits the definition of ''breach'' to a use or disclosure that ''*compromises the security or privacy''* of the PHI. The phrase ''*compromises the security or privacy*" of the PHI means that the breach ''*poses a significant risk of financial, reputational or other harm to the individual.*''

This change to the definition of "breach" from the preliminary guidance to include the "*compromises the security or privacy"* was made to ensure better consistency and alignment with State breach notification laws. Accordingly, the *Preamble* indicates that once it is established that a use or disclosure violates the *Privacy Rule*, the Health Plan must determine *whether the violation compromises the security or privacy of the PHI.*

According to HHS, to determine if an impermissible use or disclosure of PHI constitutes a breach, Health Plans and Business Associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In performing the risk assessment, Health Plans and *Business Associates* may need to consider a number or combination of factors *as* discussed at pages 6 and 7 of the *Preamble's* PDF version.

The Interim Final Rule provides a narrow, explicit exception to what compromises the privacy or security of PHI. It states that the privacy or security of PHI will not be compromised when a "limited data set" that now also excludes dates of birth and zip codes is used. HHS deemed that an improper use or disclosure of this information would not compromise the security or privacy of the PHI due to the low level of risk.

The Preamble states that Health Plans and Business Associates **must document their risk assessments**, so that if a breach occurs, they can demonstrate that notification was not required. For breaches of PHI with a low level of risk, as explained above, Health Plans will only need to document that the date disclosed did not include information that posed a significant risk of financial, reputational or other harm to the individual.

The *Preamble* notes items that the Health Plan may include in any notice to an individual whose unsecured PHI was breached (see PDF at page 12). To satisfy the notice readability requirements, a Health Plan should write the notice at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey.

Individuals responsible for a Health Plan's PHI at the Fund Office, plan professionals and *Business Associates* of the Health Plan, especially TPAs, will want to review the *Preamble* in detail and prepare draft notices and a plan of action in the event of a breach of unsecured PHI.

* * *