

ALERT
HITECH / HIPAA UPDATE:
Breach Notification Interim Final Rule Released
August 31, 2009

The interim final rule (the “Rule”) regarding the **breach notification requirements** of the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), enacted as part of the American Recovery and Reinvestment Act on February 17, 2009, were published in the Federal Register on August 24, 2009. Pursuant to the Rule and the HITECH Act, the new regulations **become effective on September 23, 2009**. Comments on provisions of this Interim Final Rule are due on or before October 23, 2009. The Rule provides more guidance on certain aspects of the HITECH ACT breach notification requirements.

Health care providers and other Covered Entities will be required to notify an individual whose unsecured protected health information (“PHI”) has been accessed, acquired or disclosed as a result of a breach of privacy or security within 60 days of the discovery of the breach, and perhaps sooner if feasible. This is a significant change from the current requirements under the HIPAA Privacy and Security Regulations which require the organization to mitigate any breach. Business Associates will be under similar reporting obligations to the Covered Entity, who in turn must notify the individual.

The content and methodology of notification is well outlined in the HITECH Act and slightly modified in the Rule. In most instances, notification will be in writing and mailed directly to the individual, unless electronic mail has been specified as a preferable means of communication by the individual. If the PHI of 500 or more Vermont residents is involved, then notification to a prominent media outlet is also required along with contemporaneous notice to the Secretary of the U.S. Department of Health and Human Services (“HHS”). The Rule makes clear that health care providers must keep a log of any breaches and annually report them to HHS not later than 60 days after the end of each calendar year.

The most difficult aspect of these new notification requirements is the breadth of the definition of “breach” as defined in the statute and clarified in the Rule:

The term “**breach**” means the acquisition, access, use, or disclosure of protected health information in a manner not permitted by Subpart E [of the HIPAA Privacy Rule] **which compromises the security or privacy** of such information.

Exceptions.

- (i) **any unintentional** acquisition, access or use of protected health information by an **workforce member or individual acting under the authority** of a covered entity or business associate if –

- (I) such acquisition, access, or use was made in **good faith** and **within the scope of his/her authority**; and
 - (II) does not result in further use or disclosure in a manner not permitted by Subpart E.
- (ii) **any inadvertent disclosure** from a person who is otherwise **authorized to access** protected health information **at a covered entity or business associate to another person authorized to access** protected health information **at same covered entity**; and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by Subpart E.
 - (iii) a **disclosure** of PHI where a covered entity or business associate has a **good faith belief** that an unauthorized person to whom the disclosure was made **would not reasonably have been able to retain such information**.

Note that the breach notification requirement does not apply if the PHI is considered “secured” such that it is rendered unusable, unreadable or indecipherable to an unauthorized individual through a methodology specified by guidance from the Secretary of HHS. While HHS has stated that securing PHI in such a manner is not required, the Rule conveys that it is best practice to do so.

The definition of **compromises the security or privacy** of PHI contained in the Rule provides more flexibility than the HITECH Act itself indicates. Specifically, the Rule provides that that phrase means “**poses a significant risk of financial, reputational, or other harm to the individual.**” Thus to determine if an impermissible use or disclosure is a breach, **health care providers must engage in 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.** The comments to the Rule lay out a series of factors to use in performing the risk assessment, ultimately concluding that it should be fact specific -- and documented.

Further, the Rule requires that covered entities must **train** all members of its workforce on these matters, provide a **process for individuals to make complaints**, refrain from taking retaliatory acts against those who do complain and to develop and impose appropriate **sanctions** for members of its workforce who fail to comply with the HIPAA Privacy Rule provisions.

Finally, HHS expressed in the Rule some sympathy for the quick compliance date of the Rule’s requirements (required by the HITECH Act). In releasing the Rule, HHS stated that, although compliance with the Rule is required on or before September 23, 2009, HHS will use its enforcement power with discretion to not impose sanctions for failure to provide required notification for breaches that are discovered before February 22, 2010 (180 days after publication of this Rule).

Other notable provisions of the HITECH Act:

Business Associates - Business Associates are clearly included in the breach notification requirements and they must notify the Covered Entity of any breach, although the burden remains with the Covered Entity to notify the individual and, as appropriate, the media and HHS.

Business Associates will become fully and directly subject to the HIPAA Privacy and Security Regulations as of February 17, 2010. Business Associate Agreements are required to be amended before that date to specifically incorporate the application of the security regulations to Business Associates.

Increased Penalties and Enforcement Authority Already Effective - The HITECH Act substantially increases the penalties that may be imposed for violations of the HIPAA Privacy and Security Regulations from the current high of \$25,000 to as much as \$1.5 million. State Attorneys General now have clear and explicit authority to enforce the HIPAA Privacy and Security Regulations. The HITECH Act also permits enforcement actions to be directed against individuals employed by a health care provider in addition to the health care provider. Beginning on February 17, 2011, fines shall be mandatory in situations involving “willful neglect” and, beginning in 2010, a “harmed” individual may share in the penalty payments recovered.

Additional Changes Effective February 17, 2010 - We expect regulations later this year to provide guidance with regard to other important HITECH provisions which will become effective on February 17, 2010, including

1. Electronic access must be provided to individuals whose PHI is part of an EHR.
2. An individual has a right to request that no disclosure of PHI be made to a Payer, and have it honored, if the individual self paid for the relevant medical care.
3. Fundraising communications must include a conspicuous statement that an individual may opt out of receiving them.
4. The Secretary of HHS is required to periodically audit Covered Entities and Business Associates for compliance with the HITECH Act and the HIPAA Privacy and Security Regulations.
5. Note that further guidance from HHS on the application of a limited data set standards to disclosures under HIPAA’s minimum necessary restrictions must be issued by August 16, 2010.

For questions or clarifications regarding these pending changes, please contact Anne Cramer at acramer@ppeclaw.com.