



[HEALTH INDUSTRY ONLINE](#) • MAY 07, 2009 • [STRASBURGER & PRICE, LLP](#)

PREPARED BY



Kevin M. Wood

600 Congress Avenue
Suite 1600
Austin, Texas 78701
512.499.3664

kevin.wood@
strasburger.com

EDITORS

David K. Meyercord
C. Scott Nichols

**HEALTH INDUSTRY
GROUP**

Tejal P. Banker
Debra W. Biehle
Thomas W. Burton
Merritt M. Clements
Kathryn Midboe Darling
William Duane Darling
Richard D. Fladung
R. Bradley Fletcher
Brian G. Hamilton
James M. Kimbell
Bryan J. Maedgen
Cynthia Schafer Marietta
David K. Meyercord
Stuart Miller
Crawford Moorefield
Craig H. Myers
C. Scott Nichols

The HITECH Act – The Privacy & Security of Health Information Still Matters

The privacy and security of health information remains a top priority for regulators. The primary federal law governing the privacy and security of health information is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Since the issuance of HIPAA's final privacy and security regulations (the Privacy Rule and Security Rule, respectively) in 2001 and 2002, few changes have been made to the HIPAA requirements.


That changed on February 17, 2009, when President Obama signed the American Recovery and Reinvestment Act of 2009 (ARRA),¹ Title XIII of which was named the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). The HITECH Act was enacted in an effort to keep pace with new threats and risks to electronically stored data, and it contains the most significant changes to privacy and security requirements since the original Privacy and Security Rules were promulgated.

Before outlining the HITECH Act changes, however, please note that the Federal Trade Commission has delayed enforcement of the Red Flags Rule (as discussed in the [previous edition](#) of *Health Industry Online*) for another 90 days. The previous enforcement deadline of May 1, 2009, **has now been extended to August 1, 2009**. Health care providers now have some additional time to determine whether they are subject to the Red Flags Rule and, if so, to develop and implement their written identity theft prevention protocols.


HITECH Act

The HITECH Act implements several new requirements that were implied, but not specified, in HIPAA. These include specific requirements for individual notification when security breaches occur, regulation of personal health record vendors, increased duties and penalties for business associates, additional limitations on the use and disclosure of protected health information (PHI), and increased

Laura Reilly O'Hara
Jeffrey S. Osgood
David L. Ovard
D. Patrick Owens
Paul W. Sheldon
John A. Tang
Joseph A. Turano
Melissa Webb
Carol D. Williamson
Ivan Wood
Kevin M. Wood

 [Printer friendly page](#)

 [View as Acrobat PDF](#)

 [Subscribe to HIO RSS](#)

enforcement efforts.

Among the major changes are strict standards for notification in the event of a security breach. The terms of the HITECH Act require covered entities—treatment providers who transmit electronic information, health plans, and health care clearinghouses—to notify individuals when the “unsecured protected health information (PHI)” has been accessed, acquired, or disclosed as a result of a breach. The notice requirement applies equally to breaches in electronic *and* paper format. The Department of Health and Human Services (HHS) is required to issue interim final rules on these notification requirements by August 2009, to become effective 30 days after publication.

One of the primary purposes of HIPAA was to spur the development and implementation of personal health records (PHR). However, HIPAA has few provisions that would regulate the privacy or security of the health information held by PHR vendors. HITECH addresses this issue by extending the notice requirements to (i) PHR vendors, (ii) entities that offer products or services through a website of a PHR vendor, and (iii) entities that access information in, or send information to a PHR vendor. The Federal Trade Commission (FTC) will govern this aspect of the HITECH Act, and the FTC is mandated to issue interim final rules for PHR vendors by August 2009.

Under HIPAA, business associates were indirectly subject to its requirements through their business associate agreements (as required by the Privacy Rule) with covered entities. Under the HITECH Act, the Privacy Rule and Security Rule requirements, and the accompanying penalties for non-compliance, have been expressly extended to business associates. Among the HITECH Act changes, business associates must now comply with the Security Rule in the same manner as covered entities. While the Security Rule now fully applies to business associates, they remain subject to the Privacy Rule through the terms of a business associate agreement. With that said, a breach of an agreement’s terms can subject the business associate to direct civil and criminal penalties.

In addition to these new requirements, the HITECH Act changes how PHI can be used or disclosed for marketing purposes. It requires specific rules governing the use or disclosure of PHI for fundraising purposes. It prohibits the sale of electronic health records (EHRs) or PHI without authorization except when the remuneration is for specific purposes. It requires HHS to issue guidance on application of the “minimum necessary” standard by August 2010. It also changes how covered entities must account for PHI disclosures, with compliance for the access and accounting requirements being phased in from January 2011 to

January 2014 (depending on when the covered entity began using EHRs).

The HITECH Act also seeks to increase HIPAA enforcement capabilities by increased penalty amounts and requiring formal investigations of potential breaches in certain cases. For example, the Secretary of HHS must conduct formal investigations of HIPAA violations that may be due to willful neglect of standards. State attorneys general may also bring civil actions in federal court if they believe that the interests of their residents have been threatened or adversely affected from a potential HIPAA violation. Civil monetary penalties have also been created based on a multi-tier approach for HIPAA violations, and these penalties went into immediate effect upon enactment of the HITECH Act:

- If the person did not know that he or she violated the law, the penalty shall be at least \$100 per violation not to exceed \$25,000 for all identical violations in a calendar year, but may be no more than \$50,000 per violation not to exceed \$1.5 million for all identical violations in a calendar year;
- If the violation occurred from reasonable cause but not willful neglect, the penalty shall be at least \$1,000 per violation not to exceed \$100,000 for all identical violations in a calendar year, but may be no more than \$50,000 per violation not to exceed \$1.5 million for all identical violations in a calendar year;
- If the violation occurred from willful neglect *and* was corrected, the penalty shall be at least \$10,000 per violation not to exceed \$250,000 for all identical violations in a calendar year, but may be no more than \$50,000 per violation not to exceed \$1.5 million for all identical violations in a calendar year; and
- If the violation occurred from willful neglect and was not corrected, the penalty shall be at least \$50,000 per violation not to exceed \$1.5 millions for all identical violations in a calendar year.

Finally, the HITECH Act is meant to clarify and supplement the HIPAA requirements, not supersede them. More specifically, the HITECH Act provides that HIPAA and its Privacy and Security Rules remain in effect to the extent they are consistent with the requirements of the HITECH Act. To ensure consistent compliance and enforcement, HHS must amend the Privacy and Security Rules by appropriate rulemaking to make them consistent with the requirements of the HITECH Act.

Health care businesses—whether covered entities, business associates, or otherwise—should evaluate their operations to determine whether they must comply with the requirements of the HITECH Act.

¹American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (2009) (ARRA).

PUBLICATIONS:

- To view past issues of Health Industry Online, please visit [Health Industry Online](#)
- To subscribe to other Strasburger publications, please visit [Strasburger Publications](#)

DISCLAIMER: Articles contained within this newsletter provide information on general legal issues and are not intended to provide advice on any specific legal matter or factual situation. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel.

ADVERTISEMENT NOTICE: This e-mail may constitute a commercial electronic mail message subject to the CAN-SPAM Act of 2003. If you do not wish to receive further commercial electronic mail messages from the sender, please send an e-mail to Strasburger@Strasburger.com and request that your e-mail address be removed from future mailings. To update your address, please send an email to Strasburger@Strasburger.com including the updated information. Strasburger & Price, LLP, 901 Main Street, Suite 4400, Dallas, TX 75202.

