



**Strasburger**  
ATTORNEYS AT LAW

## Health Industry Online

[VISIT OUR HEALTH LAW BLOG](#) • JANUARY 06, 2010 • [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  
David K. Meyercord  
Stuart Miller  
Crawford Moorefield  
Craig H. Myers  
C. Scott Nichols  
Laura Reilly O'Hara  
Jeffrey S. Osgood

## Enforcement Deadline for the HITECH Act Approaches – Is Your Organization Ready?

Enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its privacy and security regulations (the "Privacy Rule" and "Security Rule," respectively) reflected the initial attempts to move the healthcare industry into the electronic age. As noted in a prior issue of this newsletter,<sup>1</sup> few changes were made to the HIPAA requirements after adoption of the Privacy Rule and Security Rule in 2001 and 2002. That all changed in February of this year with the enactment of the American Recovery and Reinvestment Act of 2009 (ARRA),<sup>2</sup> and more specifically, Title XIII of the ARRA, which was named the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).

The new requirements imposed by the HITECH Act will have a significant impact on the privacy and security of health information and on the compliance efforts of affected healthcare entities, *including* business associate entities. While HIPAA originally applied only to covered entities—treatment providers, health plans, and healthcare clearinghouses—the HITECH Act expanded the direct applicability of the Privacy and Security Rules to business associates (*i.e.*, those service providers/vendors who provide services to or for covered entities). In fact, the primary impact of the new HITECH Act requirements will be felt by business associates, who must now develop and implement policies and procedures to demonstrate compliance with HIPAA and the HITECH Act.

Moreover, the window of opportunity for affected entities to act is shrinking. The compliance deadline for the HITECH Act changes, including the breach notification requirements, is February 17, 2010. While many of the HITECH Act changes, including compliance by affected entities, became effective in 2009, federal enforcement was delayed to allow affected entities time to adapt their operations.

If entities have not started their efforts to comply, there is no need to panic as there is still time to act. However,

David L. Ovard  
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

they must move quickly to develop and implement an appropriate plan to ensure compliance by the February 2010 deadline.

Between the expansion of HIPAA obligations to business associates and the new enforcement environment regarding privacy and security breaches, business associates have significantly more risk under the healthcare privacy framework. While covered entities will likely need to modify some of their HIPAA policies and procedures to remain in compliance, business associates will need to review the HITECH Act provisions and identify where their current compliance policies are inadequate in this new environment.

With that in mind, what are some areas that will merit attention?

### **Privacy Rule**

Of all the HITECH Act provisions, those related to the Privacy Rule present the most confusion because it is not clear that all portions of the Privacy Rule are applicable to business associates. Lack of the obligation to provide a notice of privacy practices to individuals provides just one example. Generally, however, the HITECH Act mandates that business associates, by law, must follow those portions of a business associate agreement as mandated by the Privacy Rule. While this may not present a significant shift for following existing business associate agreements, new HITECH Act rules will likely mandate revisions to such agreements, and the risks for failure to comply have grown immensely. Thus, business associates should take the opportunity to analyze whether their policies and procedures comply with the Privacy Rule.

### **Security Rule**

Unlike the Privacy Rule, compliance with the Security Rule presents much more of a challenge. In simplest terms, the HITECH Act has mandated that business associates must now maintain reasonable and appropriate security safeguards. These types of safeguards include administrative, physical, and technical safeguards as those areas are defined under the Security Rule. Because of the actual security processes mandated in each of these areas, the details will likely be quite different from what most entities use right now for reasonable security. As a result, shifting practices to implement HIPAA-compliant security standards may require significant effort. Business associates should begin this process through use of a risk analysis study as soon as possible.

### **Breach Notification**

For the first time, the HITECH Act created a federal standard for notification to individuals in the event of a security breach, whether or not the breach has anything to do with an electronic health record. While many states have similar notification requirements for identity theft purposes, the standard adopted by the HITECH Act is much broader. It applies to breaches that involve any kind of personal information held by healthcare entities and does not include any risk of harm threshold.

In August 2009, a final interim rule was adopted to implement the breach notification requirements.<sup>3</sup> When a breach of unsecured information occurs, a notice must be provided that (1) describes what happened; (2) describes the information involved; (3) lists steps the individual should take to protect themselves from potential harm from the breach; (4) includes a brief of the entity's investigation and mitigation efforts; and (5) includes the applicable contact information. The notice must be provided within 60 days of discovering the breach, and the entity must notify the Department of Health & Human Services (HHS) of the nature of the breach. If more than 500 individuals are involved, additional media notices and more stringent HHS notice timelines come into play. While the rule became effective in September 2009, enforcement will not begin until February 2010.

### **Contracting**

A major challenge will be managing the business associate agreement process, which will involve both timing and substantive matters. Healthcare entities will want to identify an appropriate strategy for this process, assess the amount of agreements involved, and determine what the agreements should say. Because of the increased enforcement risks, healthcare entities can also expect new demands and negotiation twists that will arise as each side expects different provisions to be included in the documents. While final rules and guidance from HHS on this process have not been issued, entities should prepare applicable contract language to be ready once the rules are finalized.

### **Training**

Because of the expanded nature of the required compliance efforts, business associates, in particular, will need to develop internal education and training efforts for employees. They will also need to develop an effective communication strategy for reporting breaches to customers (and affected individuals). Some of these education initiatives may be incorporated into existing training programs, but new efforts will likely be needed to

impress the seriousness of these new issues to the entity's workforce.

Because of the complexities involved with determining and maintaining HIPAA compliance, the issues listed in this discussion provide only a sample of the types of issues that healthcare entities, and more specifically business associates, must consider. While the process is manageable, it requires thoughtful analysis and an appropriate plan to respond to the many HIPAA requirements that must now be met. The sooner that process begins the more likely affected entities can meet the February 2010 deadline.

---

<sup>1</sup> See <http://www.strasburger.com/p4p/publications/The-Hitech-Act-health-information-privacy-and-security-still-matter.htm> (May 7, 2009).

<sup>2</sup> American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (2009) (ARRA).

<sup>3</sup> Breach Notification for Unsecured Protected Health Information, 74 Fed. Reg. 42740 (Aug. 24, 2009) (interim final rule) (to be codified at 45 CFR pts. 160 & 164)).

**PUBLICATIONS:**

- Subscribe to the latest health care news on Strasburger's [Health Blog](#)
- 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](mailto: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](mailto:Strasburger@Strasburger.com) including the updated information. Strasburger & Price, LLP, 901 Main Street, Suite 4400, Dallas, TX 75202.

