

HEALTHCARE LAW NEWS

BUSINESS ASSOCIATE AGREEMENTS – TIME TO UPDATE

The American Recovery and Reinvestment Act of 2009 (“ARRA”) contains the Health Information Technology for Economic and Clinical Health Act (“HITECH”). HITECH modifies HIPAA regarding privacy and security of protected health information (“PHI”).

The biggest HITECH change, in practical terms, is that HITECH *directly* regulates business associates for the first time. Previously HIPAA only indirectly affected business associates. Starting in February 2010, HITECH requires:

- Business associates must now comply directly with security rule provisions of HIPAA for electronic or e-PHI.
- Directly imposes on business associates the obligation to comply with HIPAA business associate safeguards such as limiting use and disclosure of PHI, opening their books and records to the Department of Health and Human Services, making accounting for disclosures, etc. Also, business associates are now subject to DHHS compliance audits.
- HITECH heightened privacy and security standards are also now applicable to both covered entities and business associates and require notification of security or privacy breaches, new restrictions on disclosure to health plans and enhanced civil and criminal penalties for non-compliance.

One important change is that business associates now will be deemed to have violated HIPAA if the business associates knows of a “pattern of activity or practice” by a covered entity and fails to cure the breach, terminate the business associate agreement, or report the non-compliance to the Department of Health and Human Services. In other words, your business associates have an obligation to turn you in for any violations.

Debate continues on whether all business associate agreements must be modified. While some existing business associate agreements may narrowly comply with HIPAA after HITECH, most of the business associate agreements I have reviewed recently are not adequate due to the rapidly changing rules and restrictions in this area. I strongly recommend that you review your business associate agreements to determine whether they comply with HIPAA after HITECH and make sure that the questions such as who is a business associate? Do our security guidelines adequately address disclosures? What are the procedures for accounting for disclosures? And most importantly, how have you allocated responsibility for non-compliance?

While compliance with HIPAA and now post-HITECH HIPAA has always been a moving target, and will likely change again, covered entities and business associates should work together now to develop strategies for compliance with the HITECH changes.

This newsletter is edited by Paul Wallace, a member of the American Bar Association Healthcare Law Section who has been representing physicians and healthcare practices for 30 years. Mr. Wallace assists physicians in health practices in contract items, federal legal compliance, creation of practice entities, estate and wealth planning and similar issues.

Please feel free to call if you have any questions about this newsletter or any other matter.