

# CARLTON FIELDS

ATTORNEYS AT LAW

## *HITECH Act: Business Associates Subject to Certain Provisions of HIPAA Privacy and Security Rules*

Prior to the enactment of the HITECH Act, business associates were not directly subject to the HIPAA Privacy and Security Rules. Instead, HIPAA applied only indirectly through the contractual duties and obligations imposed by the Business Associate Agreement between the covered entity and business associate. Thus, business associates were not subject to the penalties imposed by HIPAA for failure to comply with the Privacy and Security Rules; business associates only risked being held accountable for damages flowing from a contractual breach. The HITECH Act imposes dramatic changes to this dynamic, with most new requirements taking effect on February 17, 2010.

- **New Security Rule Duties and Obligations:** Section 13401(a) of the HITECH Act requires business associates to comply with certain provisions of the HIPAA Security Rule; specifically, the administrative, technical and physical safeguard requirements of the Security Rule now apply to business associates. In addition, business associates must also comply with the provision of the Security Rule requiring the implementation of security policies and procedures. If a business associate violates any of these Security Rule provisions, the business associate may be subject to the same HIPAA civil and criminal penalties previously only applicable to covered entities. See Section 13401(b) of the HITECH Act.
- **New Privacy Rule Duties and Obligations:** Section 13404(a) of the HITECH Act requires business associates to use or disclose protected health information ("PHI") only if such use or disclosure is consistent with the terms of the Business Associate Agreement between the covered entity and business associate. If a business associate violates a Business Associate Agreement with respect to this new privacy requirement, the business associate may be subject to the same HIPAA civil and criminal penalties previously only applicable to covered entities. See Section 13404(c) of the HITECH Act.
- **Entities Considered Business Associates:** Section 13408 of the HITECH Act states that any entity that provides data transmission of PHI to a covered entity, and requires access on a regular basis to such PHI, is considered a business associate and must enter into a Business Associate Agreement with each covered entity to which it provides these services. Examples include: health information exchange organizations, regional health information organizations, e-prescribing gateways, and personal health record ("PHR") vendors that provide a PHR to patients as part of a covered entity's EHR.
- **Amendment of Business Associate Agreements:** The HITECH Act requires that the new privacy and security requirements imposed on business associates be incorporated into all Business Associate Agreements, new and existing, on or before February 17, 2010.
- **Civil and Criminal Penalties:** The HITECH Act specifies that business associates will be subject to the same civil and criminal penalties previously only imposed on covered entities. As amended by the HITECH Act, civil penalties range from \$100 to \$50,000 per violation, with caps of \$25,000 to \$1,500,000 for all violations of a single requirement in a calendar year. The amount of the civil penalty imposed will vary depending on whether the violation was not knowing, due to reasonable cause, or due to willful neglect. Criminal penalties include fines up to \$50,000 and imprisonment for up to one year. In some instances, fines are mandatory.

In addition, pursuant to Section 13404(b) of the HITECH Act, a business associate must take reasonable steps to cure a breach of, or terminate, a Business Associate Agreement if it becomes aware of a pattern of activity or practice by a covered entity that violates the agreement. If a business associate fails to take reasonable steps to cure the breach, terminate the agreement, or report the problem to the Department of Health and Human Services, then the business associate may be liable for civil and/or criminal penalties under HIPAA.

For more information, please contact **Nestor J. Rivera** at 404.815.2702 or [nrivera@carltonfields.com](mailto:nrivera@carltonfields.com). For more information about Carlton Fields' Health care practice, please visit [www.carltonfields.com/healthcare](http://www.carltonfields.com/healthcare)



Nestor J. Rivera

This publication is not intended as, and does not represent, legal advice and should not be relied upon to take the place of such advice. Since factual situations will vary, please feel free to contact a member of the firm for specific interpretation and advice if you have a question regarding the impact of the information contained herein. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you free written information about our qualifications and experience.

[www.carltonfields.com](http://www.carltonfields.com)

Atlanta | Miami | Orlando | St. Petersburg | Tallahassee | Tampa | West Palm Beach