

Pierce & Mandell, P.C.
Attorneys at Law
11 Beacon Street, Suite 800
Boston, MA 02108-3002
(617) 720-2444 Fax: (617) 720-3693
www.piercemandell.com

CLIENT ALERT

September 16, 2009

**THE HITECH ACT AND
HIPAA BUSINESS ASSOCIATES**

On February 17, 2009 President Obama signed into law the American Recovery and Reinvestment Act of 2009, the Stimulus Bill. Title XIX of the Stimulus Bill is known as the “Health Information Technology for Economic and Clinical Health Act” or “HITECH Act”. Key provisions of the HITECH Act expanded HIPAA and the duties of the business associate.

Prior to the enactment of the HITECH Act, business associates were not directly subject to the HIPAA Privacy and Security Rules. Instead, HIPAA applied indirectly to business associates through contractual duties and obligations imposed by a business associate agreement between the covered entity and the business associate. Likewise, business associates were not subject to the penalties imposed by HIPAA for failure to comply with the law. The HITECH Act imposes significant changes to relationship between covered entities and business associates. These changes take effect February 17, 2010 and must be incorporated into all new and existing business associate agreements.

- Compliance with HIPAA Security Rule. The HITECH Act requires business associates comply with certain provisions of the HIPAA Security Rule, specifically the administrative, technical and physical safeguard requirements. Business associates must also implement 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.
- Compliance with HIPAA Privacy Rule. Business associates must only use or disclose protected health information (PHI) consistent with the terms of the business associate agreement. 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.
- Security Breaches and Notice. 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 (HHS), then the business associate may be liable for civil and/or criminal penalties under HIPAA.

Business associates must also notify individuals if there is a security breach of their PHI. Specifically, HHS released the HIPAA Rule in September 2009 which requires covered entities and business associates to report all breaches or disclosures of unsecured PHI. Unsecured PHI is defined as any PHI that has not been encrypted or destroyed. The HIPAA Rule requires a covered entity to notify the affected individuals without unreasonable delay, but in no case later than 60 days after discovery. The 60 day period begins on the day the covered entity first knew, or with reasonable diligence should have known about the breach.

If the business associate acts as an agent of the covered entity and performs services which would fall under the covered entity's scope of authority (e.g. billing), if a breach occurs the business associates must notify an affected individual in the same manner as a covered entity, without unreasonable delay, but in no case later than 60 day after discovery. Whereas, if the business associate acts as an independent contractors and performs an independent activity on behalf of the covered entity (e.g. data analysis), if a breach occurs then the 60 day period for notice will start when the covered entity learns of the breach.

Entities Considered Business Associates. HIPAA defines a "business associate" as an individual or entity, which is not a member of the covered entity's workforce, which performs on behalf of the covered entity any function or activity involving the use or disclosure of PHI. The HITECH Act expands the definition of business associate to also include entities that transmit PHI and require regular access to such PHI, these include: Health Information Exchange Organizations, Regional Health Information Organizations, E-prescribing Gateway, or electronic health record vendors.

All business associates must enter into business associate agreements with each covered entity to which they provide services.

- Amending 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 violation 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.

Emily Kretchmer and William Mandell represent health care providers with compliance and health information matters.