



Information Security and Privacy Management Alert

HITECH Act

The **Health Information Technology for Economic and Clinical Health Act** ("HITECH Act") is part of the American Recovery and Reinvestment Act of 2009. HITECH significantly amends the privacy and security rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") by extending the scope and imposing breach notification requirements on HIPAA-covered entities and their covered business associates. Business associates became subject to the new requirements February 17, 2010.

HITECH Act increases enforcement of and penalties for, protected health information ("PHI") privacy and security violations. Penalties and/or fines became effective with respect to breaches discovered after February 21, 2010.

Privacy and Security Rule Obligations

Privacy Rules- There are no significant new obligations or requirements under HITECH Act; however, the risks and penalties of non-compliance have substantially increased.

Security Rules-HITECH Act requires business associates to comply with HIPAA Security Rule's administrative, technical, and physical safeguard requirements and to implement security policies and procedures in the same manner as a covered entity. Before business associate were limited to safeguards that reasonably and appropriately protected confidentiality, integrity, and availability of electronic PHI. Now, a business associate needs to implement written policies and procedures that address each Security Rule standard, implement a security awareness and training program for workforce members, designate a security official, and conduct a formal, accurate and thorough security risk analysis along with a security management process.

Breach Notification Requirements

The HITECH Act's security breach notification provisions require that covered entities notify individuals if their health information has been breached. Notice is required if a company decides the incident qualified as a defined breach. Even if the access or release of information constituted a breach, a safe harbor may exist if the information was protected by the use of a technology or methodology specified in guidance from the Secretary of Health and Human Services.

If a breach is deemed to have occurred at or by a business associate, the business associate must notify the covered entity. The business associate needs to provide the covered entity with the identification of each individual affected by the breach and information required by the covered entity in its notification of the affected individuals.

It is critical for business associates to be able to identify breaches, investigate them promptly, and report them in accordance with HITECH Act. These new requirements apply to breaches involving both electronic and paper records.

Our professionals are uniquely qualified to assist you in complying with the HITECH Act Requirements and developing your information security and privacy management processes. Please contact us at 630-243-0117 or MFischer@riskinc.net.