



# **ACTION REQUIRED**

**FEBRUARY 12, 2010**

Phone: 248.355.9600

[WWW.JSCLARKAGENCY.COM](http://WWW.JSCLARKAGENCY.COM)

---

## ***COMPLIANCE WITH HITECH ACT REQUIRES – NEW BUSINESS ASSOCIATE AGREEMENT***

---

### **THE HITECH ACT APPLIES TO EVERY GROUP PLAN, REGARDLESS OF THE GROUP'S SIZE**

#### **ACTION REQUIRED:**

**Please sign and date page 5 of the attached Business Associate Agreement and return just that page to the J.S. Clark Agency. An agency representative will sign and return to you a final copy with both signatures.**

#### **BACKGROUND:**

In 1996, Congress introduced HIPAA (Health Information Portability & Accountability Act); requiring group health plans (and indirectly, their business associates) to comply with regulations to protect what the Privacy Rule\* calls Personal Health Information\*\* (PHI).

Then in 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), the government passed the Health Information Technology for Economic and Clinical Health Act (HITECH).

The provisions of HITECH expand on the protections introduced by HIPAA in 1996 by requiring direct responsibility of business associates to comply with the privacy and security of PHI as well as detailing breach notice requirements and penalties for all covered entities.

The new HITECH provisions and administration requirements impact existing HIPAA privacy and security policies for plan sponsors. Many of these requirements begin this month. Finally, the HITECH Act is applicable to every group, regardless of group size or benefit portfolio.

#### **HITECH DETAILS:**

By **February 17, 2010**, covered entities must review their existing Business Associate Agreements (BAAs) to ensure they contain provisions to comply with HITECH's new rules. The J.S. Clark Agency has provided each of our clients with a new business associate agreement (attached separately) describing the roles and responsibilities of the Agency regarding breach notification requirements, in addition to other requirements of HIPAA.

*25900 W. Eleven Mile Road, Suite 210 • Southfield • Michigan • 48034-8203*

*PHONE 248.355.9600 • FAX 248.355.3145*

*[www.jsclarkagency.com](http://www.jsclarkagency.com)*

In addition to securing new BAAs with insurance carriers, the Agency has adopted secure email encryption services through Zix Corp® to manage PHI privately and securely.

The Agency has appointed a security officer, developed written security policies and procedures and provided appropriate training to all staff members with access to PHI. We are also in the process of conducting a formal risk assessment. We have implemented the administrative, physical and technical safeguards to ensure the PHI of your group as a whole, as well as each individual, is protected and secure.

For a checklist of other items you must address to ensure compliance [CLICK HERE](#):

The HITECH provisions in ARRA focus on HIPAA privacy and security compliance. There are three specific areas driving this:

- 1) Breaches of PHI must be disclosed to affected individuals, the government and, in cases of 500 or more affected individuals, prominent media outlets.
- 2) Penalties for a breach of HIPAA's privacy and security rules have increased significantly and the federal government has stated that enforcement will be a high priority. In addition, plan sponsors can now be directly sued by a states Attorney General for HIPAA violations. [CLICK HERE](#) to view the new penalties.
- 3) Requirements on group health plans apply directly to business associates.

Under the HITECH provision, a breach is defined in the Act as “the unauthorized acquisition, access, use, or disclosure of protected health information (PHI) which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.” Furthermore, notification is required if there is an “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.”

**\*Privacy Rule**

*The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.*

**\*\*PHI (Protected Health Information)**

*According to the Department of Health and Human Services, PHI is all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI)”. Unsecured Protected Health Information – means protected health information that is not secure through the use of a technology or methodology specified by the Secretary in guidance.*