



TJ&S IS COMPLIANT WITH THE 2010 HITECH ACT REQUIREMENTS

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (“ARRA”). Included in this Act is the HITECH Act (Health Information Technology for Economic and Clinical Health Act) which makes significant changes to existing HIPAA regulations. The general effective date of the **HITECH Act** was **February 17, 2010**.

In order to comply with the new regulations set forth by the HITECH Act, TJ&S has implemented the following policies and procedures:

Business Associate Agreements

The HITECH Act requires Business Associates to comply with HIPAA regulations which previously pertained only to Covered Entities (Insurance Companies). A Business Associate is defined as: a person or entity that provides services or performs functions that involve the use or disclosure of Protected Health Information (PHI) on behalf of a covered entity.

In order to comply with the HITECH Act and to ensure that our clients and the Protected Health Information (PHI) they send to us are protected, TJ&S has obtained new Business Associate Agreements with all clients and sub-brokers.

Email Encryption

The HITECH Act requires that all electronic correspondence containing Protected Health Information (PHI) be encrypted.

In order to comply with this requirement, TJ&S has partnered with ZixCorp and implemented internal procedures to ensure that all electronic correspondence containing Protected Health Information (PHI) is sent securely through the ZixMail Email Encryption System.

Onsite Security

The HITECH Act requires that all paper correspondence and electronic files be stored in a secure location.

In response to this requirement, TJ&S has taken the following steps to ensure we are compliant:

- Paper files containing information relating to employee benefits policies are kept in locked file cabinets.
- Workstations automatically lock if not used continuously and can only be unlocked by the user assigned to that workstation.
- All documents attached to the database are encrypted and can only be viewed when accessed through the management system by a user with the appropriate access.
- In addition, our servers are housed in a locked cabinet and protected by a physical firewall as well as firewall, anti-virus, anti-spam, anti-spyware and intrusion detection software.