



## THE OBAMA ADMINISTRATION PUTS TEETH INTO THE NEW HIPAA AND HITECH LAWS AND REGULATIONS

By: Tricia Nell  
*tan@lcojlaw.com*

After years of debate, the new HIPAA legislation and HITECH regulations have become reality. The Obama Administration will be more aggressive about HIPAA enforcement than its predecessor. With this push from the White House, the health care industry can expect a rise in the number of investigations and penalties. Outlined below are three areas of the new legislation that pose issues for the health care industry.

First, the new legislation substantially increases the rule violation penalties. The maximum penalty had previously been \$25,000. This legislation suggests penalties could be up to as much as \$1.5 million. These fines are mandatory in situations involving “willful neglect.” The legislation also indicates the penalty amounts may be paid to “harmed” individuals.

Second, the security breach notification requirements have been heightened. On August 19, 2009 the US Department of Health and Human Services issued final regulations implementing the breach notification provisions of the HITECH Act of 2009 (Health Information and Technology for Economic and Clinical Health Act). The regulations went into effect on September 23, 2009 and require hospitals to notify patients and the federal government of any breaches of unsecured protected health information. The new breach reporting requirement is the first national reporting statute. It is broader and more comprehensive than any of the individual state notification laws.

For the health care industry at large, this breach notification requirement may be one of the most significant new requisites of this legislation. It could affect a large number of companies quickly and publicly. Additionally, because the notice requirement applies only to “unsecured” information, this legislation also may accelerate the movement towards encryption of a wider range of health care data.

Finally, HIPAA enforcement and penalties apply to companies that provide services to the health care industry. Each of these “business associates” must sign a contract with their health care client that extends certain HIPAA provisions to them by contract. The new provisions require the business associates to follow *all* HIPAA provisions rather than just the handful of previously required provisions. The risks for the business associates are now magnified substantially. An important point here is that this requirement is not limited to electronic health records. It extends HIPAA coverage to most business associates, whether they have anything to do with electronic health records or not.

Hospitals and health care entities need to revise all existing business associate contracts to incorporate these new requirements. Health care entities should promptly begin to develop model language and an overall approach to modification of their business associate contracts.