The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law on February 17 as part of the American Recovery and Reinvestment Act of 2009 (H.R. 1), also known as the economic stimulus bill. The legislation was designed to advance the use of health information technology, such as electronic health records.

Among other important aspects, the HITECH Act expands the scope and enforcement power of the Health Insurance Portability and Accountability Act (HIPAA), with greater penalties for non-compliance. Below is a summary of the key aspects of this new law.

Privacy and Security Regulations

HIPAA previously required that "covered entities" enter into contracts or "business associate agreements" (BAAs) with non-covered entities if those transactions involved the exchange of protected health information (PHI). The BAAs required the entities that do work on behalf of providers and insurers to use appropriate safeguards for the PHI they receive from the covered entities. The BAAs also set forth permitted uses and disclosures for the PHI. Prior to HITECH, business associates were not directly subject to either HIPAA or direct government enforcement action.

Business associates must now comply directly with the administrative safeguards, physical safeguards, policies and procedures and documentation requirements of HIPAA. Business associates also must comply with the HIPAA Privacy Rule provisions that would otherwise be applicable to them through the BAAs and any changes to the Privacy Rules whether or not those changes are covered by the BAAs. Business associates can now be subject to enforcement by federal or state authorities for any failure to comply with HIPAA (as amended by HITECH).

As opposed to the previous version of HIPAA, covered entities must now provide notice to individuals whose health information has been breached. Business associates must notify covered entities of any breaches. The covered entity must then notify the individual.

A two-part inquiry is applied for determining if notification is required:

(1) does it qualify as a "breach"; and
(2) was the information protected by encrypted technology. No notification to individuals is required if the breach-d information was covered by an encryption approved by the U.S. Department of Health and Human Services (HHS) – i.e., the information has been rendered “unusable, unreadable or in-decipherable to unauthorized individuals,” using technology or methodology approved by HHS.

Notice must occur no later than 60 days after discovery of the breach (i.e., when at least one employee of the entity knew or should have known of the breach). Notice is also required to be provided to media outlets if the information of more than 500 individuals has been compromised. Notification must also be forwarded to HHS.

**Changes To HIPAA Enforcement**

With the enactment of HITECH, HIPAA’s enforcement power is much stronger than before:

1. Criminal penalties can now be enforced against individuals, including employees of a covered entity. The scope of activities subject to criminal prosecution is broadened to include individuals who obtain or disclose individual PHI “without authorization.”

2. HITECH clarifies that HHS or state attorneys general can pursue civil penalties in cases where criminal penalties could attach but the Department of Justice declines to pursue the case. Civil monetary penalties are mandatory where a violation due to “willful neglect” has occurred.

3. HIPAA penalties will now be based on the level of the violation, with discretion given to HHS on the nature and extent of the harm. Penalties will top out at $50,000 per violation with an annual maximum of $1.5 million for repeat violations of the same provisions. HHS is precluded from imposing civil penalties (except in cases of willful neglect) if violations are corrected within 30 days.

4. HITECH expressly authorizes all state attorneys general to enforce HIPAA in federal district court. This provision gives attorneys general the power to enforce the law even if there is no state authorizing statute (but HHS reserves the right to intervene in the action). However, if the state attorney general brings the action, the penalties are the same as the former maximums under the preceding version of HIPAA – $100 per day, $25,000 annual maximum for repeat violations.

Note: This article was published in the *July/August 2009* issue of *The Employment Law Authority*. 