

What is HITECH?

By

**Lora M. Jennings
Martin, Pringle, Oliver, Wallace & Bauer, LLP**

If you have been hearing about the new HITECH requirements that went into effect February 17, 2010, for covered entities and business associates, but weren't certain about all the specifics, here are some of the key points.

1. What is HITECH?

As part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Congress enacted a wide range of new incentives for health care providers to develop and utilize electronic medical records. Congress also enacted significant privacy and security changes for covered entities and their business associates beyond issues pertaining to electronic medical records. Specifically, Congress enacted the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which enhances and strengthens the privacy and security of electronic health information under HIPAA.

2. What does HITECH require from covered entities?

Among other things, HITECH creates detailed notification requirements for covered entities and business associates when there is a breach of unsecured protected health information. Covered entities must notify each individual whose unsecured protected health information has been or is reasonably believed to have been accessed, acquired or disclosed as a result of a breach. While there are exceptions that apply, a breach is defined as the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. "Unsecured" protected health information is protected health information that is not rendered indecipherable or unusable when it is disclosed to or accessed by unauthorized individuals.

Again, while Congress sought to create incentives for health care providers to use electronic medical records, it also enacted regulations to strengthen the privacy and security of such electronic medical records. As such, covered entities that employ technology that renders protected health information unusable once the information is disclosed or wrongfully accessed will substantially reduce their liability under HITECH. Keep in mind that paper records and verbal information are also subject to the breach notification requirements. Breaches of unsecured protected health information include theft of laptops and paper records, as well as computer and network hacking incidents.

Business associates are required to notify a covered entity of any such breach of unsecured protected health information and must provide the names of the individuals whose information has been or is reasonably believed to have been accessed, acquired, or disclosed during a breach.

In addition to notifying the affected individual(s) of a breach of unsecured protected health information, covered entities must report any such breaches directly to the Secretary of Health and Human Services (“HHS”). Indeed, since the notification requirements went into effect, over forty (40) covered entities have reported breaches of unsecured protected health information to HHS, and these breaches are listed online at the Department of Health and Human Service’s website.

3. Does HITECH place any restrictions on the disclosure of a patient’s protected health information?

Pursuant to HIPAA, a covered entity must satisfy the “minimum necessary” requirement by disclosing only the minimum amount of information necessary to accomplish the purpose of the disclosure. Under the new regulations, a covered entity will be deemed in compliance with the Privacy Rule only if the covered entity limits the disclosure of protected health information to the “limited data set.” The “limited data set” is protected health information that is stripped of any identifying information. The health care provider shall determine what constitutes the minimum necessary to accomplish the intended purpose of a disclosure or use of protected health information.

In addition, HITECH does specifically allow an individual to request that her health care provider not disclose information to an insurer for payment or health care operations purposes if the patient has paid for the services out of pocket.

4. Are Business Associates affected by these new regulations?

Pursuant to these new regulations, Business Associates are now required by law to comply with the Privacy Rule and Security Rule under HIPAA. Prior to HITECH, HIPAA’s privacy rule and security rule requirements did not apply to Business Associates. The civil and criminal penalties for violations of any security provisions now apply to business associates to the same extent such penalties apply to a covered entity. Health care providers and Business Associates alike need to review their business associate contracts to incorporate these new requirements into the business associate agreement.

5 Are there any penalties for non-compliance?

HITECH significantly strengthens enforcement of the HIPAA rules. Civil penalties are now enhanced with a maximum penalty for willful neglect rising to \$1.5 million in a single year, raised from the previous high of \$25,000.00. Each state’s Attorney General is now authorized to enforce HIPAA regulations and requirements if the Attorney General has reason to believe the interest of one or more persons is threatened or adversely affected by a HIPAA violation. The Attorney General may sue to enjoin a violation or may seek damages, and may be awarded attorney fees.

Ultimately, the new requirements described above are only a portion of the provisions under HITECH. Covered entities and business associates alike face a heightened enforcement environment and should work toward ensuring compliance under HIPAA.