



HITECH BRINGS MORE AGGRESSIVE HIPAA ENFORCEMENT:

Understanding the new Healthcare Privacy and Security Rules

by J. Matthew Vines, Esquire

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) was passed as part of the American Recovery and Reinvestments Act of 2009 (ARRA or “stimulus bill”). HITECH is the most significant change to the healthcare privacy and security environment since the original Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Congress wanted to provide economic incentives to healthcare providers to implement electronic medical records, and accordingly, Congress determined that it needed to establish improved privacy and security rules for the healthcare industry. The most significant provisions of HITECH focus on notification to individuals in the event of information security breaches. For the first time, Congress enacted a national provision on breach notification directed solely at the healthcare industry.

Under HITECH, the Federal Trade Commission (FTC) and the Department of Health and Human Services (HHS) issued new security breach notification rules covering not only healthcare entities but also their business associates. HITECH is not a complete change to everything initiated by HIPAA, but the healthcare industry and all business associates have been advised to reevaluate all aspects of their HIPAA privacy and security policies.

Enforcement of the new rules is expected to increase, especially with a new tiered penalty structure with amounts ranging from \$25,000 to as much as \$1.5 million depending on the intent behind the violation. Additionally, the Attorneys General of the individual states have been given explicit authority to enforce HIPAA rules, and there is now also explicit authority for HIPAA criminal cases against employees.

In a January 8, 2010, press release, the FBI announced that Huping Zhou, a former UCLA Healthcare System researcher, pled guilty to four counts of illegally reading private and confidential medical records, mostly from celebrities and other high-profile patients. Mr. Zhou is one of the first people in the nation to be convicted of violating the privacy provisions of HIPAA. Then, on January 13, 2010, Connecticut Attorney General Richard Blumenthal announced that his office is suing Health Net of Connecticut, Inc. for allegedly failing to secure the private medical records and financial information of 446,000 Connecticut members and for allegedly delaying the reporting of a widespread security breach. The Connecticut Attorney General was the first to take legal action for a violation of HIPAA since HITECH was enacted, and in time, other states will certainly follow as they begin to diligently monitor activities

for potential violations of HIPAA. Both of these recent cases seemingly indicate that a more aggressive enforcement of HIPAA rules has begun.

HITECH puts a renewed emphasis on appropriate training, especially as a reminder to employees that privacy and security issues matter. Healthcare entities and business associates alike are expected to know how their employees are accessing and using information which places a higher premium on implementing the right policies and regularly reevaluating the details of those policies.

Most notably, HITECH creates a federal requirement for security breach notification for the healthcare industry. The federal requirement is very broad in that it applies to all protected health information (PHI) held by covered entities, and this is a fundamental change to the customer information obligations of the healthcare industry. Under the new rules, a breach is “unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.” The breach rules create a “risk of harm” threshold where there exists a significant risk of financial, reputational, or other harm to the individual.

About the author:

J. Matthew Vines, a Vice President at RSource, LLC, is a licensed attorney specializing in obtaining reimbursement on third-party payer claims for healthcare providers. Mr. Vines is a member of HFMA, AAHAM, and the American Health Lawyers Association. For additional information, Mr. Vines can be contacted at mvines@rsource.com or (202) 842-1393.

The FTC rule is available at: <http://www.ftc.gov/os/2009/08/R911002hbn.pdf>

The HHS rule is available at: [http://op.bna.com/hl.nsf/id/psts-v4rk7/\\$File/breach.pdf](http://op.bna.com/hl.nsf/id/psts-v4rk7/$File/breach.pdf)

The HITECH Act also includes several exceptions including an exception where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. A breach does not include any unintentional acquisition, access, or use of PHI by an employee if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship and if such information is not further acquired, accessed, used, or disclosed by any person.

If a breach has occurred, notification must include:

1. Description of what happened
2. Description of information involved
3. Steps the individual should take to “protect themselves from potential harm resulting from the breach”
4. Brief description of investigation and mitigation steps
5. Contact Information

Notification must be made within 60 days of breach being discovered. Under the rules, a breach “shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate.” Notably, business associates are covered and have an obligation to notify the covered entity within 60 days.

This new law extends HIPAA obligations directly to business associates – by law, not just by contract. Consequently, this law has a major impact on business associates, especially when coupled with a new enforcement environment. The major challenge facing covered entities and business associates is the apparent obligation to redo all business associate contracts to address the new requirements placed on business associates. Business associates must now follow the HIPAA Security Rule as well as the HIPAA Privacy Rule to the extent it is incorporated into required business associate contract terms. Thus, the most significant changes to business associate agreements will be the addition of provisions outlining timing and breach reporting as well as provisions related to breaches and their costs.

FTC and HHS are adamant that the changes brought about by HITECH are significant, and entities and business associates have been specifically encouraged to pursue data encryption wherever possible. FTC and HHS expected prompt compliance with HITECH, but they delayed enforcement of the new rules until February 17, 2010. Thus, there is an expectation by FTC and HHS that covered entities and business associates utilized the additional time to conduct a comprehensive evaluation of all areas that

needed improvement which means all identified changes should be in place.

With the end of the enforcement grace period as well as the recent news of the two HIPAA enforcement cases, all signs point to a more aggressive approach toward enforcing healthcare privacy and security rules.