

Putting HITECH Into Perspective

The risks and challenges associated with HITECH are not going away. Take steps now to prepare.

The risks and challenges associated with HITECH are not going away. Take steps now to prepare.

By Eric Nelson, CIPP

The HITECH Act was intended to provide assurance to the public that the privacy and security of their patient information is protected. The HITECH Act significantly expands the scope of the HIPAA Privacy and Security rules, including civil and criminal penalties, to business associates (e.g., entities providing services to health care providers, health insurers and other HIPAA "covered entities").

The HIPAA Security Rules relating to administrative, physical and technical safeguards of electronic protected health information (PHI) (plus new security requirements under the HITECH Act that apply to covered entities) now apply directly to business associates in the same way that those standards apply to covered entities .

Non-covered HIPAA entities, such as health information exchanges (HIEs), regional health information organizations and personal health record (PHR) vendors are now required to have business associate agreements with covered entities (including physicians) if they provide the electronic exchange of patient health information.

Highlights of the HITECH Act

Increased enforcement and penalties

The legislation substantially increases the civil penalty amounts based on the level and intent of a breach of privacy (e.g., whether the violation was made without knowledge; due to reasonable cause and not willful neglect; or due to willful neglect).

The legislation requires a formal investigation and imposition of civil monetary penalties for any violations due to willful neglect. While many of the HITECH final rules are not effective until after Feb. 17, 2010, the provisions on increased penalties go into effect immediately.

Security Breach Notification

Possibly the most significant of the new rules, the HITECH Act requires that covered entities must notify each patient whose *unsecured* PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, used or disclosed as the result of a breach. While previous HIPAA security requirements applied only to electronic health information, the HITECH rules apply to any form or medium of PHI. The breach notification requirements apply not only to disclosures to third parties, but to unauthorized internal access to PHI.

ALSO NEW THIS UPDATE

- [The Highs and Lows of Downtime Solutions](#)
- [ASTM Introduces Disaster Recovery Standard](#)
- [What's Your RAC IQ?](#)
- [Motivating Young IT Talent](#)

The regulations require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach "without unreasonable delay and in no case later than 60 calendar days after discovery." The 60-day clock starts on the first day that the breach is discovered by any employee or member of the workforce or on the first day that such a person reasonably should have known of the breach.

Business associates are now required to notify the covered entity of a security breach not later than 60 days after discovery of the breach, which the covered entity in turn will notify the affected individuals. If a breach affects *500 or more* individuals, covered entities are required to provide a notice in prominent media outlets in the immediate area as well as notify the Secretary of Health and Human Services, which will post the name of the breaching entity on its public Web site.

The Act also requires "vendors of personal health records" and "PHR-related entities," to notify their customers of any breach of unsecured, individually identifiable health information as well as the Federal Trade Commission (FTC).

Timeframes

Most of the provisions of the HITECH legislation take effect February 18, 2010; however, obligation to notify applies to all breaches that are discovered on or after Sept. 15, 2009, and increased penalties for HIPAA violations are effective immediately.

Challenges and Preparation

The risks and challenges associated with the HITECH Act are not going away and in fact, enforcement will continue to be more significant and substantial. Steps to prepare for HITECH compliance include:

1. Identify compliance requirements specific to your organization.
2. Perform a risk assessment that includes an inventory of PHI assets, including a thorough understanding of how PHI is collected, managed and shared as well as how it is stored, accessed and secured.
3. Identify and prioritize high risk areas and revise existing privacy and security policies and procedures to address these risks and meet compliance requirements.
4. Ensure employees and third parties receive privacy and information security training and are constantly aware of their responsibility to protect a patient's personal health information.
5. Review existing relationships between covered entities and business associates and develop a contracting and compliance strategy.
6. Develop an effective breach mitigation, detection and response plan that includes internal staff as well as third parties that collect, manage and

share PHI.

Eric Nelson is a practice leader with Lyndon Group, serving clients that have needs with privacy and information security. He is a Certified Information Privacy Professional (CIPP) and specializes in federal, state and international privacy and information security compliance and breach mitigation.

Related Articles

For more articles on HITECH, click [here](#).

Copyright ©2010 Merion Publications
2900 Horizon Drive, King of Prussia, PA 19406 • 800-355-5627
Publishers of ADVANCE Newsmagazines
www.advanceweb.com