

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009



On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 ("ARRA"). In addition to provisions designed to stimulate the economy, ARRA contains the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act" or the "Act"). The HITECH Act contains health information technology provisions and also makes significant changes to the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA Privacy and Security Rules"). The general effective date of the HITECH Act is **February 17, 2010**, but many provisions have varying effective dates and must be reviewed carefully.

This issue of the Lambert & Carney Benefits Group LLC. Legislative Brief provides you with an overview of the changes to the HIPAA Privacy and Security Rules imposed by the HITECH Act.

Business Associates

The HIPAA Privacy and Security Rules currently apply to Covered Entities: health plans, health care providers and health care clearinghouses. Under current law, a Covered Entity's Business Associates must agree, through a Business Associate Agreement, to comply with certain requirements of the HIPAA Privacy and Security Rules, but are not directly regulated by the regulations. The HITECH Act makes a number of these requirements directly applicable to Business Associates. In addition, penalties for violations of the Privacy and Security Rules that formerly applied only to Covered Entities will now apply to Business Associates as well.

Business Associates will now be required to comply directly with many provisions of the HIPAA Privacy Rules that currently apply to Covered Entities. The obligations that were previously required to be included in the Business Associate Agreement, such as using Protected Health Information ("PHI") only for permitted purposes and using appropriate safeguards, are now directly applicable to Business Associates. In addition, Business Associates that become aware of breaches of the Privacy Rule by a Covered Entity are required to take steps to cure the breach. If they are unsuccessful, they must terminate the agreement or notify the Secretary of Health and Human Services ("HHS"). This responsibility must be included in the Business Associate Agreement.

Business Associates must also comply with the HIPAA Security Rules. The additional obligations must be incorporated into the Business Associate Agreement between the Covered Entity and Business Associate. The Act also provides that, each year, HHS must issue guidance on the most effective and appropriate technical safeguards for use in compliance with the HIPAA Security Rule.

The HITECH Act also expands the definition of Business Associate to include organizations that provide data transmissions of PHI to a Covered Entity (or its Business Associate) and require access on a routine basis to such PHI, as well as vendors that contract with Covered Entities to offer a Personal Health Record to patients. These Business Associates must enter into Business Associate Agreements with the Covered Entities.

The new requirements for Business Associates are effective on **February 17, 2010**.

Security Breach Notification

Covered Entities do not currently have a specific obligation to report breaches of privacy or security of PHI. The HITECH Act will require Covered Entities to notify individuals whose "unsecured PHI" has been breached. If the breach involves PHI held by a Business Associate, the Business Associate must notify the Covered Entity.

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

The notification must be made without unreasonable delay and no later than 60 days after the discovery of the breach. Generally, the notification must be provided by first class mail but can also be provided by e-mail, if the individual has specified a preference to receive notices electronically. The Covered Entity must also provide notice to “prominent media outlets” if the breach affects more than 500 individuals in a state or jurisdiction. Covered Entities must notify HHS of all breaches. Notice must be provided immediately for breaches involving more than 500 individuals and annually for all other breaches. HHS will post breaches involving more than 500 individuals on its website (www.hhs.gov).

The Act requires the notice to include the following information:

- A description of the breach, including the date of the breach and date of discovery;
- The type of PHI involved (such as full name, Social Security number, date of birth, home address or account number);
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- Steps the Covered Entity is taking to investigate the breach, mitigate losses and protect against future breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, e-mail address, website or postal address.

The Act does not specify when PHI is considered to be “secure” but directs HHS to issue guidance regarding which technologies are considered secure within 60 days of the Act’s enactment. In the event timely guidance is not issued, “unsecured PHI” will mean PHI that is not secured by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals. HHS is also required to issue interim final regulations governing the notification requirement within 180 days of enactment. The notification requirement will apply to breaches discovered on or after the date that is **30 days after the regulations are issued**.

The Act also imposes a temporary breach notification requirement on vendors of personal health records (“PHR”) and other non-HIPAA Covered Entities. PHR vendors must notify any individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of a breach of security. PHR vendors must also notify the Federal Trade Commission (“FTC”), which will in turn notify HHS. Any third party service provider that provides services to a PHR vendor and discovers a breach, must notify the vendor. Violations of this requirement will be treated as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act. The FTC is required to issue interim final regulations regarding this requirement within 6 months of enactment and the requirement will be effective **30 days after the regulations are issued**.

Individual Rights

Accounting for Disclosures

The HIPAA Privacy Rule requires a Covered Entity to provide an individual with an accounting of disclosures of PHI upon request, but permits routine disclosures for treatment, payment or health care operations to be excluded from the accounting. The new law extends HIPAA’s requirement to provide that, if a Covered Entity maintains an “electronic health record” for an individual, the Covered Entity must account for disclosures through the electronic

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

health record for treatment, payment or health care operations as well. This additional disclosure accounting is limited to a period of three years prior to the request.

An electronic health record is defined as an electronic record of health-related information on an individual that is created, gathered, managed or consulted by authorized health care clinicians and staff.

The effective date for this provision depends on when the electronic health record is held by the Covered Entity and appears to give current users of electronic health records additional time to update their systems. For electronic health records held by a Covered Entity as of January 1, 2009, the disclosure accounting requirement would apply to disclosures on or after **January 1, 2014**. For electronic health records held after January 1, 2009, the requirements apply on or after **January 1, 2011**, or the date the electronic health record is acquired, whichever is later. However, these dates may be delayed to 2016 and 2013 respectively.

Access to Electronic Health Records

In addition to being able to access PHI held by a Covered Entity as required by the HIPAA Privacy Rule, an individual is permitted under the HITECH Act to access PHI in an electronic health record in electronic form. The Covered Entity may charge the individual for the cost of labor for providing access. An individual may also direct the Covered Entity to transmit the electronic health record directly to another person or entity. This provision is effective on **February 17, 2010**.

Right to Restrict Disclosures

Under current law, an individual may request that a Covered Entity not disclose the individual's PHI, even if the disclosure would be for treatment, payment or health care operations. However, the Covered Entity is not required to agree to the restrictions. The HITECH Act will require Covered Entities to agree to an individual's request to restrict disclosures to a health plan for payment or health care operations if the PHI pertains to services or treatment that have been paid out of pocket and in full. This provision is effective on **February 17, 2010**.

Restrictions on Disclosure

The HITECH Act contains several new restrictions on the disclosure of PHI.

Prohibition on Sale of Protected Health Information

Under the Act, Covered Entities and Business Associates may not receive remuneration for the disclosure of PHI without the individual's authorization. There are limited exceptions for disclosures for public health, treatment or research purposes. Payment for research purposes is limited to the cost of preparing and transmitting the data. HHS is required to issue regulations implementing these new restrictions within 18 months. The new rule will become effective **six months after the regulations are issued**.

Marketing Restrictions

Certain marketing communications that were permissible under the HIPAA Privacy and Security Rules are no longer permitted under the HITECH Act. Pursuant to the new rule, Covered Entities and Business Associates may not use PHI to inform an individual about the Covered Entity's products or services without the individual's authorization if the Covered Entity receives compensation from another party for making the communication. This new rule does not apply in cases where the communication involves a drug the individual is already taking and where any compensation

Legislative Brief

LAMBERT & CARNEY
BENEFITS GROUP, LLC

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

for that communication is reasonable in amount or where the communication is made by a Business Associate on behalf of a Covered Entity and is consistent with the terms of the business associate agreement.

Minimum Necessary Standard

In general, Covered Entities are required to use or disclose the “minimum necessary” amount of PHI. Currently, there is little guidance as to what constitutes the minimum amount necessary and Covered Entities were required to make this determination on their own. The HITECH Act requires HHS to issue regulations **within 18 months of enactment** regarding the minimum necessary requirement. Until then, Covered Entities must use or disclose only a limited data set, if it is sufficient for the intended purpose. A limited data set excludes certain identifying information but is not fully de-identified.

Penalties and Enforcement

Civil Penalties

HHS may currently conduct compliance reviews to determine whether a Covered Entity is in compliance with the HIPAA Privacy and Security Rules. The Act also requires HHS to perform periodic audits of Covered Entities to ensure their compliance.

Currently, HHS may assess civil penalties of \$100 per violation of the Privacy and Security Rules, up to \$25,000 for violations of each requirement during a calendar year. The HITECH Act increases the amounts of the civil penalties that may be assessed and distinguishes between the types of violations. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. HHS is also required to assess penalties for violations involving willful neglect and to formally investigate complaints of such violations.

For violations where the individual does not know of the violation, the minimum penalty remains \$100 per violation, up to \$25,000 per calendar year for identical violations. If the violation is due to reasonable cause, the minimum penalty is \$1,000 per violation, up to \$100,000 per calendar year. For corrected violations that are caused by willful neglect, the minimum penalty is \$10,000 per violation, up to \$250,000 per calendar year. The maximum civil penalty for any type of violation and the minimum penalty for violations caused by willful neglect that are not corrected is \$50,000 per violation, up to \$1.5 million per calendar year for identical violations.

The updated civil penalty amounts apply to violations occurring after **February 17, 2009**. Other enforcement provisions apply to penalties that are imposed **24 months after the date of enactment**. HHS is required to issue regulations governing the enforcement provisions within 18 months of enactment.

The Act requires the General Accounting Office to review methodologies for allowing a portion of civil penalties to be paid to affected individuals. HHS must establish a methodology by **February 17, 2012**.

State Attorneys General are authorized by the Act to bring civil actions against Covered Entities to enjoin further violations and obtain damages on behalf of residents of their states, if HHS has not already taken action. The amount of damages is up to \$100 per violation, with a maximum of \$25,000 per calendar year for identical violations. This provision is effective for violations occurring any time after **February 17, 2009**.

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

Criminal Penalties

The new law does not change the criminal penalties that may be assessed for violations of the Privacy and Security Rules. Those penalties remain \$50,000 and one year in prison for knowing violations, \$100,000 and five years in prison for violations committed under false pretenses and \$250,000 and 10 years in prison for offenses committed for commercial or personal gain.

Under the Act, criminal actions may be brought against anyone who wrongly discloses PHI, not just Covered Entities or their employees. Also, the Act gives HHS (in addition to the Department of Justice) the authority to bring criminal actions against these individuals.

Please contact your Lambert & Carney Benefits Group LLC. representative at (800) 357-1840 with any questions.

This Lambert & Carney Benefits Group LLC. Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

EM 2/09



1375 Kings Highway East, Suite 215, Fairfield, CT 06824
Phone: (800) 357-1840
Fax: (203) 292-8179