

NEWS FLASH

IMPORTANT INFORMATION REGARDING HIPAA

A Stradley Ronon Publication

MARCH 2009

Stimulus Bill Expands HIPAA Privacy and Security Rules

Stradley Ronon Stevens & Young, LLP
2600 One Commerce Square
Philadelphia, PA 19103
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Malvern, Pa.
Harrisburg, Pa.
Wilmington, Del.
Cherry Hill, N.J.
Washington, D.C.



www.meritas.org

Our firm is a member of Meritas – a worldwide business alliance of more than 200 law offices in 66 countries that offers high-quality legal services through a closely integrated group of independent full-service law firms.

Information contained in this publication should not be construed as legal advice or opinion or as a substitute for the advice of counsel. The enclosed materials may have been abridged from other sources. They are provided for educational and informational purposes for the use of clients and others who may be interested in the subject matter.

Copyright © 2009
Stradley Ronon Stevens & Young, LLP
All rights reserved.

The economic stimulus legislation, known as the American Recovery and Reinvestment Act of 2009 (ARRA), contains extensive changes to the privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA). ARRA significantly expands the privacy and security provisions of HIPAA that are applicable to covered entities and business associates, and provides for increased enforcement and penalties for noncompliance. It also expands individuals' rights regarding disclosure of their protected health information (PHI). A brief summary of the most significant HIPAA changes is set forth below.

Business Associates Now Subject to HIPAA Privacy and Security Rules

Before ARRA was enacted, only covered entities – such as health plans and health care providers – were subject to the HIPAA privacy and security rules. Business associates of covered entities were not subject to these rules. A business associate is any person or entity who performs or helps perform a function or activity on behalf of a covered entity that involves the use or disclosure of PHI. Third-party administrators, utilization reviewers and attorneys who represent covered entities are among the parties who are frequently treated as business associates. Effective February 17, 2010, business associates will be subject to the HIPAA privacy and security rules.

As a result of ARRA, business associates will now be subject to civil and criminal

penalties and to enforcement proceedings for violations of the HIPAA privacy and security rules. In addition, ARRA will require business associates to appoint a security official, develop written HIPAA policies and procedures, and train their workforce on how to protect PHI. Further, business associates will need to implement physical and technical safeguards to limit access to and protect the security of PHI. In addition, all existing business associate contracts must be reviewed and amended not later than February 17, 2010, to incorporate the changes that will be needed to satisfy the requirements of the HIPAA changes enacted by ARRA.

Individual Rights

ARRA provides that, within 30 days after guidance is issued by the Department of Health and Human Services (HHS), individuals who are affected by a breach of the privacy and security of their PHI must be notified of that breach. Prior to ARRA, there was no requirement that individuals be notified of such a breach. If the breach of PHI involves a business associate, the business associate must notify the covered entity of the breach. Covered entities must notify any individual affected by a breach of unsecured PHI, retain logs of such breaches and submit the logs to HHS annually. HHS must be notified of privacy or security breaches involving more than 500 individuals. If 500 or more individuals who are affected by the breach live in the same geographic area, the breach must be reported to the local media.

continued on back



Stradley Ronon Stevens & Young, LLP
2600 One Commerce Square
Philadelphia, PA 19103

Attn: Cheryl Jackson

Under ARRA, individuals will have the right to an accounting of disclosures of PHI made through electronic records by covered entities or their business associates for treatment, payment or health care operations. If a covered entity uses or maintains electronic health records that contain PHI, an individual may request a copy of his or her records in electronic format or may direct the covered entity to send a copy to another entity or person. With regard to electronic health records held by a covered entity as of January 1, 2009, the new accounting requirement will apply to disclosures on or after January 1, 2014. With respect to electronic health records acquired after January 1, 2009, the accounting requirement will apply to disclosures on or after January 1, 2011.

New Enforcement Rules and Penalties

ARRA requires HHS to audit covered entities and their business associates regarding HIPAA privacy and security compliance, and to formally investigate a covered entity (or a business associate) upon receipt of a complaint.

The Act authorizes state attorney generals to institute civil enforcement actions in federal court against any person whose HIPAA violations pose a threat to or harm one or more residents of the state. It also significantly increases the amount of civil penalties for HIPAA violations. Prior to ARRA, the penalty was \$100 per violation, up to a maximum amount of \$25,000 for multiple violations in the same calendar year. Under ARRA, penalties can range, depending on the type of violation, from \$100 to \$50,000 per violation, with a cap of \$25,000 to \$1.5 million per year for violations of an identical requirement during the same calendar year. A portion of any penalty assessed under HIPAA will be distributed to individuals harmed by the violation. The remainder of the penalty will be transferred to the HHS Office for Civil Rights for use in enforcing HIPAA. HHS is required to issue regulations relating to these enforcement provisions by August 17, 2010.

If you have any questions or need further information regarding the new HIPAA privacy and security rules, please contact John J. Hunter at (215) 564-8072 or JHunter@Stradley.com. ■

