



Garfunkel, Wild & Travis, P.C.

New York New Jersey Connecticut

# Legal Alert

ADVERTISING MATERIAL

March 2009

## Significant New HIPAA Provisions in the Recent Economic Stimulus Package

The recently enacted American Recovery and Reinvestment Act of 2009 (the "Stimulus Package") provides over \$19 billion dollars to promote the adoption of electronic medical records. However, the decision to promote electronic medical records in the health care industry raised significant concerns about the privacy and security of the health information in those records. Accordingly, Congress also included in the Stimulus Package substantial changes to the privacy and security requirements of the Federal Health Insurance Portability and Accountability Act ("HIPAA"). These changes will require all HIPAA covered entities to revise their policies and procedures and reevaluate some of their existing security and privacy practices. In addition, Business Associates will now directly be liable under HIPAA and will likely need to develop new policies and procedures.

Briefly, some of the significant privacy and security requirements of the Stimulus Package include:

1. New Security Breach Reporting Requirements. Covered Entities are required to notify individuals of security breaches involving their protected health information ("PHI"), unless the PHI is secured in a way that makes it unusable, unreadable or indecipherable. Unlike many state notification laws, this new rule applies to breaches involving any of an individual's PHI, not just social security numbers or credit card numbers. In addition, Business Associates are required to notify a Covered Entity of a security breach involving the Covered Entity's PHI. Notices must be made without unreasonable delay and in no case later than sixty (60) days after the discovery of the breach by anyone in the organization. The new rules contain specific requirements regarding the content and manner of giving notices to individuals.
2. Notices to Media. There are special notice requirements for breaches involving more than five hundred (500) residents of a State or other jurisdiction. In such cases, notice must be provided to prominent media outlets (e.g., newspapers, radio, etc.) serving the State or jurisdiction.
3. Notices to the Secretary of the Department of Health and Human Services ("DHHS"). Covered Entities must provide notice to the Secretary of DHHS whenever PHI has been acquired or disclosed in a breach unless the PHI has been appropriately secured to prevent access (e.g., through encryption). If the breach involves 500 or more individuals, notice to the Secretary must be provided immediately. For all other breaches, Covered Entities may maintain a log of breaches and report them to the Secretary annually. The Secretary will post on the DHHS website a list of each Covered Entity involved in a breach involving more than 500 individuals.
4. Business Associates. Most of the HIPAA security regulations will now apply to Business Associates directly in the same manner as they apply to Covered Entities. In addition, the Business Associate requirements of the privacy regulations will apply directly to Business Associates, and Business Associates will be required by law to use and disclose PHI only in compliance with the Business Associate Agreement. Finally, Business Associates will now be subject to civil and criminal penalties for privacy and security violations.
5. Accountings. Under the pre-existing privacy regulations, Covered Entities are not required to provide individuals with accountings of disclosures made for treatment, payment or health care operations. However, under the new rules, Covered Entities will be required to account for disclosures of PHI in electronic health records made for purposes of treatment, payment or health care operations. Accountings must be provided for any such disclosures made during the three (3) years prior to the date on which the accounting is requested.

*continued...*

6. Prohibitions on the Sale of PHI. With certain exceptions, Covered Entities and Business Associates will be prohibited from directly or indirectly receiving remuneration in exchange for any PHI of an individual unless the Covered Entity has obtained a valid authorization from the individual. Any such authorization must specify that PHI can be exchanged for remuneration.
7. Marketing. The new privacy rules narrow substantially the circumstances under which Covered Entities may use PHI for marketing purposes. For example, there are strict limitations on the ability of a Covered Entity to make marketing communications when it has received direct or indirect payment in exchange for marketing.
8. Increased Enforcement Provisions. The Stimulus Package includes provisions that greatly increase the limits on civil monetary penalties that can be imposed for HIPAA violations. Further, under the new rules, the Secretary of DHHS is required to impose a civil penalty for all HIPAA violations arising from willful neglect. The Secretary is also required to formally investigate any complaint if a preliminary investigation of the facts indicates a possible violation due to willful neglect. Finally, the new rules permit civil enforcement of HIPAA by State Attorney Generals.

\* \* \* \* \*

Covered Entities and Business Associates must take notice of these new HIPAA requirements. Many of the new privacy and security requirements will become effective on February 17, 2010, although the increased penalty provisions go into effect immediately and certain provisions requiring the adoption of implementing regulations will take two years or longer to go into effect. According to the Stimulus Package, the Secretary of DHHS will be promulgating guidance and additional regulations that will further strengthen HIPAA requirements. Covered Entities and Business Associates must review their privacy and security policies to ensure that they will meet these new requirements. GWT is available to advise clients about the necessary steps to maintaining compliance with HIPAA's requirements. If you require any assistance or want to learn more about the GWT HIPAA program, please call any of the attorneys at GWT.

\* \* \* \* \*

If you have any questions, please contact the GWT attorney with whom you regularly consult.

## About Garfunkel, Wild & Travis, P.C.

Garfunkel, Wild & Travis, P.C. was founded in 1980 with a single purpose in mind: to become a pre-eminent health care law firm attending to the unique business and legal needs of its clients. Since then, the firm has grown to over 80 attorneys devoted to addressing the complex legal, regulatory, business and financial needs of its diverse clients.

If you would like to receive Legal Alert mailing from Garfunkel, Wild & Travis, P.C. electronically in the future, or if you would like to be removed from the mailing list, please contact us at (516) 393-2258 or [subscriptions@gwtlaw.com](mailto:subscriptions@gwtlaw.com). You may also visit the Firm's website at [www.gwtlaw.com](http://www.gwtlaw.com).

THIS MATERIAL IS INTENDED AS INFORMATIONAL ONLY AND THE CONTENT SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. READERS SHOULD NOT ACT UPON INFORMATION IN THIS MATERIAL WITHOUT FIRST SEEKING PROFESSIONAL ADVICE.

PLEASE BE ADVISED THAT PURSUANT TO NEW JERSEY RULE OF PROFESSIONAL CONDUCT 7.3(B)(5), WE ARE REQUIRED TO PROVIDE THE FOLLOWING NOTICES:

NOTICE: BEFORE MAKING YOUR CHOICE OF ATTORNEY, YOU SHOULD GIVE THIS MATTER CAREFUL THOUGHT. THE SELECTION OF ANY ATTORNEY IS AN IMPORTANT DECISION.

NOTICE: IF THIS LETTER IS INACCURATE OR MISLEADING, REPORT SAME TO THE COMMITTEE ON ATTORNEY ADVERTISING, HUGHES JUSTICE COMPLEX, P.O. BOX 037, TRENTON, NEW JERSEY 08625.