LAW·FLASH
A CLIENT ALERT FROM THE EMPLOYEE BENEFITS PRACTICE
Morgan Lewis
COUNSELORS AT LAW
www.morganlewis.com

HIPAA Triple Play: Privacy, Security and Enforcement

March 14, 2006

2006 marks the 10th anniversary of the passage of HIPAA, and this spring brings a HIPAA privacy reminder, the application of HIPAA security rules to small plans and the finalization of HIPAA enforcement rules for HIPAA violations.

As a consequence of this springtime HIPAA triple play, employers of every size will have to complete new HIPAA tasks. Further, all employers should review their HIPAA compliance strategy and business associate agreements to ensure that their HIPAA strategy is viewed as favorably as possible under the new enforcement rules.

Privacy
Group health plans are required to maintain a Notice of Privacy Practices that provides information about how protected health information is used or maintained by the group health plan and describes individuals' rights with regard to their health information. Plans that initially complied with the Notice obligation by April 14, 2003 (which was the Notice compliance date for all but small plans) must remind participants by April 14, 2006 that the Notice is available and must inform participants how to obtain the Notice. While many employers have reminded participants about HIPAA Privacy Notices, it is critical that employers determine whether the reminder complied with HIPAA procedures. For example, electronic Notice dissemination or reminders must meet particular HIPAA standards that may be problematic for employers with retail or manufacturing operations.

Security
HIPAA security rules for covered entities with small plans are effective April 20, 2006. These security rules are identical to the 2005 security rules for large plans and represent an expansion and refinement of the security rules first found in the earlier HIPAA privacy rules. (See http://www.morganlewis.com/pubs/hipaa2.pdf for our 2005 HIPAA Security Rule Webinar Material.)

By April 20, 2006, small plans possessing electronic protected health information must have examined their administrative, technical and physical safeguards and specifically implemented policies and procedures for electronic protected health information that comply with the security rules' standards, implementation specifications and other requirements.

As important as the actual policies and procedures are clear documentation and a specific written risk analysis of the security rule standards and implementation specifications. Even when an implementation specification is addressable instead of required, if the small plan will not be implementing the specification or will be implementing an alternative method, the risk analysis must capture why the

specification is not reasonable for the small plan and whether there is an equivalent alternative that is reasonable and appropriate.

Enforcement
On February 16, 2006, the Department of Health and Human Services issued a final rule addressing HIPAA enforcement. The final rules have been expanded beyond their initial application to HIPAA privacy and now address all HIPAA administrative simplification requirements, including the security and transactions and code sets. The final rule is similar to rules proposed last year, and is effective March 16, 2006.

Now, with the finalization of the HIPAA enforcement rule, the Department is empowered to assess civil monetary penalties for HIPAA violations. The penalty of $100 per violation may reach $25,000 per year for violations of an identical requirement or prohibition.

However, the rule emphasizes that the Department is still primarily focused on voluntary compliance with HIPAA and will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with HIPAA. Further, factors considered in applying any civil monetary penalty include the nature, time period and circumstances of the violation. Significantly, the rule also states that a covered entity is not responsible for a business associate's violations provided that the covered entity had a current and sufficient business associate agreement and did not know of a pattern of improper activity of the business associate or, if it did, it acted in accordance with its obligation to cure a breach.

As a consequence of the final rule, it is clear that the steps an employer takes to satisfy the documentation requirements of HIPAA will be critical components in the determination of whether the Department applies a civil monetary penalty. Sufficient and accurate HIPAA Privacy Notices, business associate agreements and security written risk analyses, along with quick and responsive interactions with the Department, will go a long way toward reducing or eliminating any civil monetary penalties.

How We Can Help
Morgan Lewis attorneys are well versed in these and other HIPAA requirements applicable to your plans. We have helped many employers examine the impact of HIPAA, create and implement training policies, negotiate business associate agreements, prepare plan documents and execute and document written risk analyses for HIPAA security rules. If you would like any assistance with these requirements, please reach out to one of the attorneys listed below to discuss how the HIPAA triple play will impact your business this spring.

If you would like further information regarding the issues raised in this Morgan Lewis LawFlash, please contact any of the following Morgan Lewis attorneys:

Chicago

David Ackerman	312.324.1170	dackerman@morganlewis.com
Andy R. Anderson	312.324.1177	aanderson@morganlewis.com
Brian D. Hector	312.324.1160	bhector@morganlewis.com

Dallas

Riva T. Johnson	214.466.4107	riva.johnson@morganlewis.com
John A. Kober	214.466.4105	jkober@morganlewis.com
Erin Turley	214.466.4108	eturley@morganlewis.com

New York
Craig A. Bitman 212.309.7190 cbitman@morganlewis.com
Gary S. Rothstein 212.309.6360 grothstein@morganlewis.com

Philadelphia
Robert L. Abramowitz 215.963.4811 rabramowitz@morganlewis.com
Brian J. Dougherty 215.963.4833 bdougherty@morganlewis.com
I. Lee Falk 215.963.5616 ilfalk@morganlewis.com
Robert J. Lichtenstein 215.963.5726 rlichtenstein@morganlewis.com
Joseph E. Ronan, Jr. 215.963.5793 jronan@morganlewis.com
Steven D. Spencer 215.963.5714 sspencer@morganlewis.com
Mims Maynard Zabriskie 215.963.5036 mzabriskie@morganlewis.com

Pittsburgh
John G. Ferreira 412.560.3350 jferreira@morganlewis.com
R. Randall Tracht 412.560.3352 rtracht@morganlewis.com

San Francisco
Mark H. Boxer 415.442.1695 mboxer@morganlewis.com
Eva P. McComas 415.442.1249 emccomas@morganlewis.com

Washington, D.C.
Jessica R. Bernanke 202.739.5447 jbernanke@morganlewis.com
Althea R. Day 202.739.5366 aday@morganlewis.com
Margery S. Friedman 202.739.5120 mfriedman@morganlewis.com
Gregory L. Needles 202.739.5448 gneedles@morganlewis.com

About Morgan, Lewis & Bockius LLP
Morgan Lewis is a global law firm with more than 1,200 lawyers in 20 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo and Washington, D.C. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.