Morgan Lewis

alert

employee benefits lawflash

www.morganlewis.com

HITECH Ushers in Era of Higher Penalties Under HIPAA

March 3, 2011

Two recent actions by the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) suggest we have entered a new era of more stringent enforcement of the privacy and security standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Covered entities, particularly those in the healthcare industry, should be vigilant in their HIPAA compliance efforts in order to avoid paying sizeable penalties.

For the first time, OCR, which is charged with enforcing HIPAA's privacy and security standards, has imposed a civil money penalty under HIPAA. In a press release dated February 22, 2011, OCR announced that Cignet Health of Maryland was fined a total of $4.3 million for ignoring requests for medical records from 41 individuals and for failing to cooperate with OCR's investigation of 27 related complaints.

Two days later, OCR announced a $1 million settlement with Massachusetts General Hospital after an employee left documents containing patients' health information on the subway. OCR's investigation indicated that the hospital "failed to implement reasonable, appropriate safeguards to protect the privacy of protected health information." As part of the settlement, the hospital agreed to issue new HIPAA policies and procedures and conduct employee training.

HIPAA originally capped penalties at $100 per day and $25,000 for the same violation in any one year. HHS investigated complaints in its discretion and entered into compliance agreements, but was criticized for not doing enough to enforce HIPAA.

In 2009, the Health Information Technology and Clinical Health Act (HITECH) significantly increased the potential monetary penalties for HIPAA violations to a minimum of $100 and a maximum of $50,000 per day, up to a maximum of $1.5 million for the same violation in any one year. In addition, HITECH requires OCR to investigate complaints and perform compliance audits and authorizes state attorneys general to enforce HIPAA.

The new penalty scheme provides for tiered penalty amounts based on the nature and extent of the violations, the nature and extent of the resulting harm, and the violator's history of compliance, among other factors. OCR has stated that the failure of an organization to implement adequate privacy and

security policies and procedures may cause investigators to conclude that the organization has a higher level of culpability, which may result in a higher penalty.

In the Cignet Health case, OCR imposed the minimum penalty of $100 per day for each failure to respond to patients' requests for medical records. However, OCR assessed the maximum penalty of $50,000 per day (capped at $1.5 million per year) for Cignet's failure to cooperate with OCR's investigation, including ignoring a subpoena.

In connection with its settlement agreement with Massachusetts General Hospital, the director of OCR, Georgina Verdugo, said, "We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement."

Covered entities in the healthcare industry are obvious targets of OCR's stepped-up enforcement efforts; however, all covered entities, including employer-sponsored health plans, can learn important lessons from OCR's actions. These cases demonstrate the importance of the following:

- Adopting adequate written privacy and security policies and procedures
- Training employees on HIPAA's requirements
- Monitoring compliance and acting quickly to mitigate any damage resulting from a breach
- Cooperating with OCR investigations

Even the minimum penalties under HIPAA can add up quickly and, by its recent actions, OCR has indicated that it will not tolerate a lack of seriousness when it comes to HIPAA compliance by covered entities.

For information about HITECH-compliant HIPAA privacy and security policies and procedures and employee training programs appropriate for your organization, please contact any of the Morgan Lewis attorneys listed below.

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

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	215.963.4812	bdougherty@morganlewis.com
I. Lee Falk	215.963.5616	ilfalk@morganlewis.com
Amy Pocino Kelly	215.963.5042	akelly@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
David B. Zelikoff	215.963.5360	dzelikoff@morganlewis.com
Pittsburgh		
Lisa H. Barton	412.560.3375	lbarton@morganlewis.com
John G. Ferreira	412.560.3350	jferreira@morganlewis.com
Lauren B. Licastro	412.560.3383	llicastro@morganlewis.com
R. Randall Tracht	412.560.3352	rtracht@morganlewis.com
Washington, D.C.		
Althea R. Day	202.739.5366	aday@morganlewis.com
Benjamin I. Delancy	202.739.5608	bdelancy@morganlewis.com
David R. Fuller	202.739.5990	dfuller@morganlewis.com
Mary B. (Handy) Hevener	202.739.5982	mhevener@morganlewis.com
Gregory L. Needles	202.739.5448	gneedles@morganlewis.com
Palo Alto		
S. James DiBernardo	650.843.7560	jdibernardo@morganlewis.com
Zaitun Poonja	650.843.7540	zpoonja@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

IRS Circular 230 Disclosure

To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein. For information about why we are required to include this legend, please see http://www.morganlewis.com/circular230.