Morgan Lewis

alert

employee benefits lawflash

March 21, 2012

HIPAA/HITECH Enforcement Action Alert

Health plan agrees to pay $1.5 million following HHS investigation of self-reported data breach.

If you report a significant data breach to the Department of Health and Human Services (HHS), you may face a follow-up investigation and possible enforcement action.

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires entities covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals. HHS pays close attention to these breach reports and initiates investigations of those it deems significant, as evidenced by its recently announced settlement with BlueCross BlueShield of Tennessee (BlueCross).

In 2009, BlueCross reported the theft of 57 unencrypted computer hard drives containing the protected health information (PHI) of more than one million customers from a former BlueCross call center in Chattanooga. The hard drives had been stored in a network data closet that BlueCross continued to lease after it had otherwise vacated the office space. The closet was secured by biometric and keycard scan security with a magnetic lock and an additional door with a keyed lock. In addition, the property management company for the leased spaced provided security services.

In spite of these physical safeguards, HHS determined that the PHI contained on the hard drives was not protected well enough. In addition to paying a penalty of $1.5 million, BlueCross agreed to a corrective action plan that requires it to, among other things, submit its HIPAA privacy and security policies and procedures to HHS for review and approval, distribute the policies and procedures to all members of its workforce who have access to PHI, report violations of the policies and procedures by members of the workforce to HHS within 30 days, train all current workforce members on the approved policies and procedures and all new workforce members within 40 days of hire, and submit to unannounced site visits.

We encourage all HIPAA-covered entities (including health plans, healthcare providers, and healthcare clearinghouses) and their business associates to take a fresh look at the HIPAA privacy and security safeguards they have in place and to employ all reasonable means of securing PHI. It is worth noting that had the hard drives been encrypted (i.e., secured), BlueCross would not have been obligated to report the theft under HITECH. The less unsecured PHI that exists, the less opportunity there is for a reportable breach that may lead to an HHS investigation and penalties.

Contacts

For information about the firm's HIPAA Privacy Compliance Initiative, please contact Lauren Licastro (412.560.3383; llicastro@morganlewis.com), Georgina O'Hara (215.963.5188; go'hara@morganlewis.com), or Sage Fattahian (312.324.1744; sfattahian@morganlewis.com), or any of the following Morgan Lewis attorneys:

Chicago

Andy R. Anderson	312.324.1177	aanderson@morganlewis.com
Saghi (Sage) Fattahian	312.324.1744	sfattahian@morganlewis.com

New York

Craig A. Bitman	212.309.7190	cbitman@morganlewis.com

Philadelphia
Robert L. Abramowitz 215.963.4811 rabramowitz@morganlewis.com
Georgina L. O'Hara 215.963.5188 go'hara@morganlewis.com
Steven D. Spencer 215.963.5714 sspencer@morganlewis.com

Pittsburgh
Lauren B. Licastro 412.560.3383 llicastro@morganlewis.com

San Francisco
W. Reece Hirsch 415.442.1422 rhirsch@morganlewis.com

Washington, D.C.
Althea R. Day 202.739.5366 aday@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 start-ups—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.