
FDA & Healthcare LawFlash

January 8, 2013

OCR Reaches \$50,000 Settlement with Hospice for Small Data Breach

Enforcement action sends a strong message to the healthcare industry and reaffirms the need for security risk analysis and mobile-device security policies and procedures.

On January 2, the U.S. Department of Health and Human Services (HHS) announced its first settlement for a security breach involving fewer than 500 patients under the Health Insurance Portability and Accountability Act (HIPAA). The HHS Office for Civil Rights (OCR) reached a \$50,000 settlement and two-year corrective action plan with the Hospice of North Idaho (HONI), resulting from a stolen unencrypted laptop computer containing the electronic protected health information (ePHI) of 441 patients.

The settlement is significant because it reaffirms, consistent with other recent OCR actions, that HIPAA-covered entities, regardless of the size of the organization, should conduct a formal security risk analysis and implement policies and procedures with respect to mobile-device security. Based on its investigation, OCR noted that HONI had failed to conduct a security risk analysis or adopt mobile-device policies and procedures. In its press release,¹ OCR emphasized the importance of encrypting data, noting that it is “an easy method for making lost information unusable, unreadable and undecipherable.”

In reaching this settlement, OCR noted that it is sending “a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients’ health information.” The \$50,000 resolution amount is less than other recent OCR settlements with larger organizations, suggesting that OCR may take the size of the entity into account in crafting a settlement.

In its press release, OCR also highlighted its new educational initiative, *Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information.*² which offers practical tips for healthcare providers and organizations on ways to protect ePHI when using mobile devices, such as laptops, tablets, and smartphones. Because breaches are often caused by the loss or theft of mobile devices, HIPAA-covered entities would be well served to develop security policies and procedures specifically addressing this risk area.

The HONI settlement demonstrates that even smaller HIPAA-covered entities, and even those as seemingly sympathetic as a small not-for-profit hospice organization, may be subject to OCR enforcement actions. Since the September 2009 compliance date of the Health Information Technology for Economic and Clinical Health (HITECH) Act interim final breach notification rule, OCR has received thousands of mandated reports with respect to breaches involving fewer than 500 patients. The HONI settlement suggests that OCR may be combing through even these smaller breach notifications for potential settlements and enforcement actions.

Contacts

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

1. View the press release at <http://www.hhs.gov/news/press/2013pres/01/20130102a.html>.

2. For more information on the initiative, visit <http://www.HealthIT.gov/mobiledevices>.

Morgan Lewis

Washington, D.C.

Howard J. Young

202.739.5461

hyoung@morganlewis.com

San Francisco

W. Reece Hirsch

415.442.1422

rhirsch@morganlewis.com

Heather Deixler

415.442.1317

hdeixler@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, 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.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change. © 2013 Morgan, Lewis & Bockius LLP. All Rights Reserved.