DechertOnPoint

July 2008 / Special Alert

A legal update from Dechert's Employee Benefits and Executive Compensation and Health Law Groups

First-Ever Monetary Settlement Reached for HIPAA Violation

On July 17, 2008, the Department of Health and Human Services ("DHHS") announced that it had entered into a Resolution Agreement with Seattle-based Providence Health & Services ("Providence") to settle potential violations of the Privacy and Security Rules. As part of this Agreement to resolve potential violations stemming from lost and stolen computers containing health information, Providence agreed to pay $100,000 and to implement a detailed corrective action plan to "ensure that it will appropriately safeguard identifiable electronic patient information against theft and loss."

Although the HIPAA Privacy and Security Rules have been effective since April 2003 and April 2005, respectively, this has been the first monetary settlement DHHS has entered into for any violations of these Rules. Instead, the Office of Civil Rights ("OCR"), charged with enforcing the Privacy Rule, and the Centers for Medicare and Medicaid Services ("CMS"), responsible for enforcing the Security Rule, have resolved thousands of privacy and security rule complaints simply by requiring entities to make changes to their health information privacy and security practices.

According to the DHHS press release, the incidents giving rise to the Agreement involved two entities within the Providence Health System: Providence Home and Community Services and Providence Hospice and Home Care. On several occasions in 2005 and 2006, backup tapes, optical disks, and laptops containing unencrypted electronic protected health information were removed from Providence premises and left unattended. The media and laptops were subsequently lost or stolen, compromising the protected health information of over 386,000 patients. HHS received over 30 complaints about the stolen tapes and disks. These complaints were submitted after Providence informed patients of the theft, as required under state notification laws.

Under the Resolution Agreement, Providence agreed to pay a $100,000 resolution amount, which technically is not considered a civil money penalty. Providence also agreed to implement a "robust" corrective action plan that requires Providence to:

- Revise its policies and procedures regarding physical and technical safeguards (*e.g.*, encryption) governing off-site transport and storage of electronic media containing patient information, subject to DHHS approval;
- Train workforce members on the safeguards;
- Conduct audits and site visits of facilities; and
- Submit compliance reports to DHHS for a period of three years.

According to Kerry Weems, acting administrator of CMS, "This resolution confirms that effective compliance means more than just having written policies and procedures. To protect the privacy and security of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training, and physical and technical features."

All HIPAA covered entities should review and/or complete their HIPAA Security Rule compliance programs. Given the Resolution Agreement described above, the fact that CMS hired PricewaterhouseCoopers to conduct a series of HIPAA security compliance reviews (reported in our January 2008 *DechertOnPoint*), and how ubiquitous security breaches have become, hospitals and health plans should consider reviewing their safeguards and risk management strategies.

Special attention should be paid to policies and practices relating to remote access, storage, and transmission of electronic protected health information. Although the HIPAA Security Rule does not require the use of encryption, the Resolution Agreement described above nonetheless indicates that not encrypting electronic protected health information may no longer be considered reasonable under certain circumstances.

■ ■ ■

Dechert has the expertise to assist both health care providers and employer health plans in reviewing and conducting risk analyses as well as reviewing policies and practices. If you would like to discuss your HIPAA compliance strategy, please call the Dechert attorney with whom you regularly work or any of the attorneys listed.

Practice group contacts

If you have questions regarding the information in this legal update, please contact the Dechert attorney with whom you regularly work, or any of the attorneys listed.
Visit us at www.dechert.com/employeebenefits and www.dechert.com/health.

Robert W. Ballenger
Philadelphia
+1 215 994 2208
robert.ballenger@dechert.com

David F. Jones
Chair, Employee Benefits and Executive Compensation
Philadelphia
+1 215 994 2822
david.jones@dechert.com

Susan M. Hendrickson
Princeton
+1 609 620 3206
susan.hendrickson@dechert.com

Beth L. Rubin
Philadelphia
+1 215 994 2535
beth.rubin@dechert.com

Teresa L. Salamon
Philadelphia
+1 215 994 2273
teresa.salamon@dechert.com

Dechert LLP

www.dechert.com

U.S. Austin • Boston • Charlotte • Hartford • Newport Beach • New York • Philadelphia Princeton • San Francisco • Silicon Valley • Washington, D.C. • **EUROPE** Brussels London • Luxembourg • Munich • Paris • **ASIA** Hong Kong