alert Health Practice

Saul Ewing LLP

JULY 2013

HIPAA security violations result in $1.7 million settlement

Authors:
Bruce D. Armon
Karilynn Bayus

SUMMARY

On July 8, 2013, WellPoint, Inc., a managed care company ("WellPoint"), agreed to pay a $1.7 million fine to settle a self-reported breach of HIPAA, a key federal health privacy law, that led to the unauthorized disclosure of the electronic protected health information ("ePHI") of approximately 612,000 individuals. The breach occurred because WellPoint did not adequately secure its information systems when making changes. The settlement with the U.S. Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR") reminds all entities covered by HIPAA to use caution when updating their information systems.

What happened?

The OCR's investigation was triggered by WellPoint's self-reporting of a breach of the Health Information Portability and Accountability Act of 1996 ("HIPAA"). The OCR's subsequent investigation revealed that from October 23, 2009 through March 7, 2010:

- WellPoint did not adequately implement policies and procedures for protecting access to the online application database under HIPAA's Security Rule;
- WellPoint did not perform an appropriate technical evaluation in response to its software upgrade to determine compliance with the Security Rule; and
- WellPoint did not implement technology to verify the identity of individuals accessing ePHI it maintained on the database.

To settle the matter, HHS-OCR entered into a Resolution Agreement with WellPoint. (Read the agreement at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf) In announcing this Agreement, HHS noted in its press release that, "This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet."

Other examples of HIPAA enforcement

The WellPoint Resolution Agreement is the latest of a series of actions by OCR with respect to HIPAA violations:

- In June 2013, the Shasta Regional Medical Center agreed to a fine of $275,000 for HIPAA violations. The OCR investigation was prompted by a newspaper article in which representatives of Shasta Regional Medical Center met with the media to discuss services provided to a patient without a valid written authorization.

- In May 2013, Idaho State University ("ISU") agreed to pay $400,000 to settle alleged HIPAA Security Rule violations. ISU self-reported a breach of unsecured ePHI for approximately 17,500 patients.
- In December 2012, the Hospice of North Idaho ("HONE") agreed to pay $50,000 to settle alleged HIPAA Security Rule violations. HONE self-reported a breach of an unencrypted laptop that was stolen and this resulted in the first settlement involving a breach of unsecured ePHI affecting fewer than 500 individuals.

HIPAA compliance challenges

Health care providers, health plans and other HIPAA-covered entities face complex challenges in complying with HIPAA, particularly in light of ever-changing technological advancements. Required breach disclosures under HIPAA heighten the stakes to ensure compliance.

Covered entities must be mindful that on September 23, 2013, the revised HIPAA regulations released in January 2013 shall go into effect. These revised rules will impact covered entities and business associates. Given the regulatory changes, OCR's enforcement efforts, and mandatory HIPAA breach reporting pursuant to the Health Information Technology for Economic and Clinical Health ("HITECH") Act, it is essential for all covered entities and business associates to ensure that they are HIPAA compliant at all times, including when implementing changes to information systems.

Saul Ewing attorneys have substantial experience in advising clients on HIPAA privacy and security issues, reviewing and implementing HIPAA compliance programs, and working with clients on breach reporting. If you have any questions about this Client Alert or would like more information, please contact Bruce Armon or Karilynn Bayus, one of the other attorneys in the Health Practice, or the attorney in the firm with whom you are regularly in contact.

This Alert was written by Bruce D. Armon, a member of the firm's Health Practice and Managing Partner of the Philadelphia office, and Karilynn Bayus, a member of the firm's Health Practice. Bruce can be reached at 215.972.7985 or barmon@saul.com. Karilynn can be reached at 215.972.1892 or kbayus@saul.com.