$400K settlement for failure to update HIPAA business associate agreement

Rick L. Hindmand | Monday, September 26, 2016

On September 23, 2016, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced an expensive reminder, in the form of a $400,000 settlement, of the need to review and update business associate agreements (BAAs) to incorporate all terms required under the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

Background

Care New England Health System (CNE) entered into the settlement on behalf of covered entities under its common ownership and control for failure to update business associate agreements between CNE and the covered entities to comply with revisions under the HIPAA Omnibus Rule. CNE provides various corporate and administrative support functions for its affiliated covered entities, including Woman & Infants Hospital of Rhode Island (WIH), which notified OCR in 2012 of the loss of backup tapes containing ultrasound studies.

During the course of its investigation of the breach, OCR discovered that the 2005 business associate agreement between WIH and CNE had not been updated to reflect the Omnibus Rule. The Omnibus Rule, which was issued in 2013 and generally required compliance by September 23, 2013, allowed a grandfather period (through September 22, 2014) for covered entities and business associates to update existing business associate agreements if certain conditions were satisfied.

OCR determined that WIH violated the Privacy and Security Rules from September 23, 2014 (when the grandfather period expired), through August 28, 2015 (when the business associate agreements were finally updated as a result of OCR's investigation), by disclosing protected health information (PHI) to its business associate (CNE) and allowing CNE to access PHI without obtaining a compliant business associate agreement. In addition to the $400,000 payment, the Resolution Agreement requires CNE and its covered entity affiliates to implement a Corrective Action Plan.

WIH previously agreed to pay $150,000 under a 2014 consent judgment with the Massachusetts Attorney General's Office for failure to implement appropriate safeguards for the backup tapes and to timely notify individuals of the breach. While noting that the Massachusetts actions did not legally preclude OCR form imposing civil monetary penalties for underlying breach, OCR determined that potential violations relating to the breach had already been addressed by the Massachusetts consent judgment, so OCR did not include those potential violations in calculating the settlement amount.

Takeaways

This settlement confirms that OCR views failure to update a previously valid business associate agreement to comply with the 2013 Omnibus Rule as a serious violation of the HIPAA Privacy and Security Rules. OCR is continuing its focus on business associate agreements, following a string of three recent OCR settlements within the last 10 months holding covered entities responsible for failing to enter into business associate agreements with their business associates:

- $750,000 - Raleigh Orthopaedic Clinic, P.A.
- $1.55 million - North Memorial Health Care
- $3.5 million - Triple-S Management Corporation

Corporate affiliates need to recognize when their arrangements involve business associate relationships and therefore require business associate agreements. This is the second OCR settlement within the last three months based on business associate relationships among affiliates. In late June 2016, OCR announced its first HIPAA resolution agreement with a business associate, which in that case was the parent of the covered entities.

In light of escalating enforcement based on business associate relationships, it is becoming even more important for covered entities and business associates to identify their business associate relationships, confirm that appropriate business associate agreements are in place, and update their business associate agreements as needed to reflect HIPAA requirements as well as appropriate business terms.

To learn more about HIPAA compliance and keeping your business and patient information protected, contact the attorney listed below.

Rick L. Hindmand