Semanoff Ormsby Greenberg & Torchia, LLC
Business Lawyers Serving Business People

Health Information Privacy & Security Update

Spring/Summer 2016

Our firm represents health care providers ("covered entities") and their business associates who handle, have access to, or transmit protected health information ("PHI".) In the last month alone, we have reviewed business associate agreements ("BAA"s) for multiple clients engaged to provide services to covered entities. The execution of a BAA is more than a mere check-the-box paperwork exercise. Likewise, covered entities should know to whom they are handing PHI and obtain adequate assurances that the privacy and security of the information will be safeguarded or risk significant penalties in the event of breach.

U.S. Department of Health and Human Services Office for Civil Rights Enforcement Settlements

Within the last two months, the Office for Civil Rights ("OCR") announced three new settlements with significant monetary payments to the government. On March 16 and March 17, 2016, OCR announced settlements with North Memorial Health Care of Minnesota ($1.55 million) and Feinstein Institute for Medical Research ($3.9 million), respectively. Both settlements emanated from the organization self-reporting the theft of an unencrypted laptop computer containing electronic protected health information ("ePHI".)

When OCR investigated North Memorial Health Care's breach report involving Accretive (its payment and operations contractor.) OCR concluded that North Memorial Health Care failed to have a business associate agreement ("BAA") in place with Accretive as required under HIPAA. OCR also found that North Memorial Health Care failed to complete a comprehensive security risk analysis. To settle the allegations of non-compliance, North Memorial Health Care agreed to a settlement of $1.55 million and an onerous corrective action plan lasting two years from the date North Memorial Health Care puts in place all required documents under the required corrective action plan.

This settlement is significant in that it emphasizes the importance of having business associate agreements in place. It should be noted that the stolen laptop incident and the commencement of OCR's investigation occurred prior to the extension of HIPAA's reach (and OCR's enforcement authority) to business associates. Thus, the covered entity was in OCR's cross-hairs for the actions of its business associate. If this incident occurred today, the focus of OCR may well be on the business associate directly rather than the health care covered entity, assuming that the healthcare entity could produce a compliant BAA with the business associate. Failure to have that business associate

agreement in place can open up the covered entity to OCR's scrutiny of its organization-wide compliance based on an action or incident isolated to the business associate.

In the OCR settlement involving Feinstein Institute for Medical Research, a biomedical research institute headquartered in Manhasset, New York, OCR's investigation found that Feinstein's security management process was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the entity. OCR also found numerous and significant deficiencies in the policies and procedures and safeguards employed by the entity. For these findings, Feinstein agreed to pay OCR $3.9 million and entered into a three-year corrective action plan. The Feinstein Institute settlement highlights that research entities are not excluded from the requirements of HIPAA. A covered entity should evaluate its involvement with research organizations as carefully as it does other entities and vendors to assess the research entity's understanding of HIPAA compliance and to ensure the appropriate authorizations or other agreements are in place as required under HIPAA.

On April 14, 2016, OCR entered into a settlement with Raleigh Orthopaedic Clinic, PA, of North Carolina. Raleigh Orthopaedic agreed to pay $750,000 to settle charges that it violated HIPAA by turning over PHI to a potential business partner without having executed a business associate agreement. Raleigh is a provider group practice that operates clinics and an orthopaedic surgery center. OCR's investigation indicated that Raleigh Orthopaedic released x-ray films and related PHI to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopaedic failed to execute a BAA with this entity prior to turning over the x-rays containing PHI.

The U.S. Department of Health and Human Services Office for Civil Rights Enforcement Ramps Up its audit of Covered Entities

Phase 2 of HIPAA Audits Underway

On the heels of these three significant settlements, OCR announced the long-awaited (but not longed for) start to Phase 2 of the HIPAA Privacy, Security, and Breach Notification Audit Program. OCR has sent out (via email) letters to a pool of entities requesting verification of contact information. OCR advises entities to check their junk or spam filters for emails from OCR which will come from OSOCRAudit@hhs.gov. After the contact information is verified, OCR will send a questionnaire to a pool of potential audit candidates and will categorize entities based on size, type, operations (public or private, affiliation with other organizations, etc.) and geographic factors. From that pool, OCR will "randomly" select its first **audit targets** in a manner that ensures a cross section of the industry. Approximately 200 organizations will be audited in the first round, which will be desk audits only – unless findings are so bad they need to come on site.

The first round of desk audits is slated to be completed by December 31, 2016. **From there, OCR will audit business associates and begin a round of on-site audits.** Our firm represents both covered entities and their business associates. If any of our clients receive a contact verification letter, and surely if they receive a questionnaire, they should promptly begin assembling their policies around the topics identified for the initial desk audits (e.g., security risk assessments, individual access to PHI and timing and content of breach notification letters, for starters). If selected for audit, an entity will have only 10 days to submit the required information to OCR. OCR has not signalled any intention to grant extensions. Covered entities may want to consider conducting a self-audit in preparation for the real deal – eventually OCR will come calling.

HIPAA Compliance Risk Areas

Speaking from the podium at a recent national conference at which OCR announced the beginning of the Phase 2 audits, OCR discussed the "lessons learned" from recent investigations. These lessons learned should serve as a road map for covered entities in reviewing their HIPAA compliance. Here are the top five takeaways:

1. Conduct a comprehensive risk analysis. OCR has high expectations for a true risk analysis. The assessment should be comprehensive and enterprise-wide covering all sources and locations of PHI. It should identify the vulnerabilities of the organization. Organizations should use the results of the risk assessment to create a risk mitigation plan.
2. Both paper records and portable devices continue to cause problems. While on opposite ends of the technology spectrum, both unsecured paper records and unencrypted portable devices are the cause of a number of breaches. OCR indicated some organizations may be leaving paper records out of compliance policies or risk assessments. While portable devices continue to be a significant source of breach, OCR's message is: don't forget about the paper!
3. Make sure your paper documents are HIPAA-compliant documents. OCR discussed that they have seen a number of non-compliant forms used for patient authorizations. Patient authorization forms are used for requested uses and disclosures of PHI not authorized by the Privacy Rule. This form requires the inclusion of specific elements to be HIPAA-compliant.
4. Confirm business associate agreements are in place. OCR continues to see that not all covered entities have business associate agreements with their business associates. Large and small organizations alike have countless business associate relationships. Covered entities should consider tracking the flow of data and payments made outside the organization to capture any missed business associate relationships.
5. Pay close attention to individual rights under HIPAA. In particular, OCR has signalled a new focus on an individual's right to access their own health information. OCR has recently added

comprehensive guidance on patients' right to access their PHI, timeliness requirements, costs that can be charged to a patient, and when access can be denied. Some of the expectations included in the document give new detail and direction to access requirements and limitations that may have been more loosely interpreted in the past. Covered entities should carefully review the guidance and the organization's access policies now that OCR has shined a light on this area of the Privacy Rule. They are most certainly signalling heightened enforcement of these provisions.

For more information on health privacy and security, please contact us 215.887.0200 or jhenshell@sogtlaw.com

www.sogtlaw.com
2617 Huntingdon Pike, Huntingdon Valley, PA 19006 | 140 East Butler Avenue, Chalfont, PA 18914