KROKIDAS & BLUESTEIN
ATTORNEYS

HEALTH CARE CLIENT ALERT

THREE IMPORTANT HIPAA UPDATES

This Alert is to remind entities subject to HIPAA of the following:

1. **All Business Associate Agreements dated before January 26, 2013 must comply with the Omnibus HIPAA Final Rule (the "Omnibus Rule") by September 22, 2014.**

The Omnibus Rule, which was enacted on March 26, 2013, became effective September 23, 2013. The Omnibus Rule required covered entities to ensure that their HIPAA policies and forms were up-to-date, and that any internal changes to HIPAA practices were properly implemented with appropriate training. The Omnibus Rule required covered entities and business associates (including subcontractors) operating under business associate agreements (BAAs) dated on or before January 25, 2013, to comply with the Omnibus Rule by September 22, 2014.

Accordingly, covered entities and business associates operating under BAAs entered into prior to January 26, 2013 (which were not otherwise renewed or modified from March 26, 2013 to September 22, 2013), must review their existing BAAs, and, if necessary, execute new BAAs, to ensure compliance by September 22, 2014. In order to comply with the Omnibus Rule, the BAAs must, among other things, (i) state that the Security Rule and certain Privacy Rule requirements extend to Business Associates, and (ii) reflect updated breach notification provisions.

To review K&B's summary alert on the Omnibus Rule, including changes to the BAAs, click here: http://www.kb-law.com/articles/documents/alert-2013-08-06-REMINDER-COVERED-ENTITIES-MUST-PREPARE-FOR-SEPTEMBER-23-2013-HIPAA-OMNIBUS-COMPLIANCE-DATE.pdf

2. **The U.S. Department of Health and Human Services, Office of Civil Rights (OCR) to Begin Phase 2 of HIPAA Audit Program**

OCR has announced that it will begin a second phase of audits relating to privacy, security and breach notifications, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. OCR conducted Phase 1 of the Audit Program

from 2011 to 2012 with a focus on covered entities. Phase 2 of the Audit Program will include both covered entities and business associates.

For Phase 2, OCR will randomly select a pool of up to 800 covered entities and issue a mandatory pre-audit screening survey. The pre-audit survey will address organization size and location, services provided, and contact information. The survey is also expected to request from covered entities the names, addresses and contact information for their business associates. Based on the responses, OCR will select approximately 350 covered entities for the Phase 2 Audit Program. OCR will also select the business associates that will participate in the Phase 2 Audit Program from this group.

Instead of a comprehensive review of HIPAA compliance, the Phase 2 Audit Program will focus on areas of particular risk to the security of protected health information (PHI) and areas of noncompliance based on OCR's Phase 1 audit findings and observations. The Phase 2 Audit Program also is intended to identify best practices and uncover risks and vulnerabilities that OCR has not identified through other enforcement activities. OCR will use the Phase 2 Audit Program findings to identify areas where it should develop technical assistance for covered entities and business associates. In circumstances where an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited organization that could lead to civil monetary penalties.

3. The Massachusetts Attorney General Issues Its First Monetary Settlement with a Covered Entity Under State Data Breach Laws

The HITECH Act empowers state attorney generals to bring civil actions for breaches of HIPAA. This summer, the Massachusetts Attorney General's Office (AGO) brought an action under HIPAA and applicable state laws, including the Massachusetts Data Security Law (201 CMR 17.00, et seq.) against Women and Infants Hospital of Rhode Island, after unencrypted back-up tapes containing information on more than 12,000 Massachusetts patients went missing. The Hospital failed to report the missing tapes for six months. As a result of the breach, the AGO and the Hospital entered into a settlement agreement, whereby the Hospital agreed to pay a fine of $150,000, conduct a compliance review and issue a report based on the review to the AGO, comply with more aggressive reporting time frames for three years, and comply with other administrative and training requirements. See: http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-07-23-women-infants-hospital.html

Covered entities, business associates, and subcontractors should take necessary steps, such as risk assessments and reviews of current policies and procedures, to ensure compliance with both the Omnibus Rule and the Massachusetts Data Security Law.

Please contact any of the following members of Krokidas & Bluestein's health care team with questions or if you would like assistance with HIPAA compliance: Anjali Waikar (awaikar@kb-law.com); Emily Kretchmer (ekretchmer@kb-law.com); Braden Miller (bmiller@kb-law.com); Jennifer Gallop (jgallop@kb-law.com); Anthony Cichello (ajc@kb-law.com); and Robert Griffin (rgriffin@kb-law.com).