KROKIDAS & BLUESTEIN
ATTORNEYS

CLIENT ALERT

OMNIBUS HIPAA FINAL RULE & OTHER HIPAA DEVELOPMENTS

On January 17, 2013, the Office of Civil Rights of the United States Department of Health and Human Services (HHS) released the Omnibus HIPAA Final Rule (the "Omnibus Rule"). The Omnibus Rule is based, in part, on statutory changes under the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

In general, the Omnibus Rule increases the privacy protections afforded consumers and the penalties imposed on organizations for noncompliance. Organizations should ensure that their HIPAA policies and forms are up-to-date, and that any internal changes in HIPAA practices are properly implemented with appropriate training.

The following is an overview of some of the important changes under the Omnibus Rule. Defined terms are as used in HIPAA.

Effective Date

The Omnibus Rule becomes effective March 26, 2013. Covered Entities and Business Associates have 180 days, or until September 23, 2013, to comply. However, we recommend updating your organizational HIPAA policies and procedures well in advance of this date.

Business Associates

Definition Expanded.

1. The Omnibus Rule clarifies that the definition of Business Associates includes not only entities that create, receive or transmit personal health information (PHI), but also entities that "maintain" PHI. This means that entities which possess or store PHI for Covered Entities on a random or infrequent basis, such as off-site email servers, are Business Associates, even if they do not access or view the PHI.

2. The definition now includes subcontractors. This confirms that Business Associates and their subcontractors are directly subject to HHS's Office of Civil Rights' enforcement action for HIPAA compliance.

3. The definition now includes Health Information Organizations, e-prescribing gateways, Patient Safety Organizations and persons that offer Personal Health Records.

Timeline: Business Associate Agreements that were in place as of January 25, 2013 will be grandfathered until September 22, 2014. Business Associate Agreements entered into or amended from and after January 26, 2013 should be amended prior to September 23, 2013 to comply with the Omnibus Rule.

Notice of Privacy Practices

As of September 23, 2013, the following statements must be included in an organization's Notice of Privacy Practices (NPP):

- the types of uses and disclosures that require authorization (e.g., marketing, disclosure of psychotherapy notes, as appropriate, etc.), including a statement relating to the prohibition on the sale of PHI without the express written authorization of the individual;

- where the organization communicates with an individual to raise funds, the right of the individual to opt out of receiving such communications;

- the right of an individual to restrict disclosures of PHI to a health plan where the individual pays out-of-pocket for his or her services in-full; and

- the right of the affected individuals to be notified of a breach of unsecured PHI (e.g., a simple statement of the right to receive notification in the event of a breach).

The Omnibus Rule eliminates the requirement that the NPP contain a separate statement about appointment reminders, information about treatment alternatives and other health-related benefits and services.

Breach Notification

The Omnibus Rule eliminates the "harm" standard for assessing when a breach requires notification.

Current Standard: a breach which poses a "significant risk of financial, reputational, or other harm" to the affected individual must be reported.

New Standard: there is now a presumption that an unpermitted acquisition, access, use or disclosure of PHI is reportable, unless the organization can demonstrate that there is a low probability that the information has been compromised.

The new standard provides organizations with less discretion in determining whether or not to report an impermissible use or disclosure of PHI. Most breaches are likely to require notification.

Risk Assessments: In assessing breaches against the new notification standard, organizations should consider, at a minimum, the following factors:

- the nature and scope of the PHI involved;
- the identity of the party who received or used the PHI;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the confidentiality of the PHI has been mitigated.

If, after considering these factors, the organization fails to demonstrate a low probability that the PHI has been compromised, notification of the breach is required.

Individual Rights

The Omnibus Rule increases the privacy rights of individuals, including:

- The right to restrict disclosure of the individual's PHI to a health plan if –
  - the disclosure is for payment or health care operations and is not otherwise required by law; and
  - the PHI pertains solely to a health care item or service for which the individual (i.e. not the health plan) has paid the provider in full.
- The right to access PHI electronically, if requested.

Organizations may consider including these additional rights in their NPP.

Enforcement / Audit Protocol

The Omnibus Rule retains HIPAA's tiered civil monetary penalty structure, with a few modifications, including a more stringent standard that requires HHS's Office of Civil Rights to investigate any complaint where possible noncompliance with HIPAA is due to willful neglect.

Organizations should be aware of a recent HHS enforcement action which suggests that the federal government is taking its enforcement power seriously. HHS recently entered into a $50,000 settlement with an organization regarding a HIPAA breach involving **fewer than 500 individuals**. The breach incident involved a stolen laptop containing information about 441 patients. The penalty was imposed in part because HHS determined that the provider failed to conduct an accurate and through risk analysis relating to its electronic security management and did not adequately adopt or implement security measures for portable devices. For HHS's press release about the settlement, click here; for a copy of the Resolution Agreement between HHS and the organization, including the Corrective Action Plan, click here.

HHS also recently issued a comprehensive audit protocol, available here. The protocol provides a useful checklist for ensuring that your organization's policies and procedures are HIPAA-compliant.

More Information

We will provide additional guidance with respect to the Omnibus Rule over the coming months. For the HHS Press Release about the Omnibus Rule containing a summary of its important provisions, click here.

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