PATTON BOGGS LLP

January 22, 2013

HHS Issues HIPAA Omnibus Final Rule

HEALTH CARE CLIENT ALERT

This Alert provides only general information and should not be relied upon as legal advice. We would be pleased to discuss our experience and the issues presented in this Alert with those contemplating investments in these markets. For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Kathleen J. Lester
202.457.6562
klester@pattonboggs.com

Stephen P. Nash
303.894.6173
spnash@pattonboggs.com

Karen Smith Thiel, Ph.D.
202.457.5229
kthiel@pattonboggs.com

Melodi M. Gates
303.894.6111
mgates@pattonboggs.com

WWW.PATTONBOGGS.COM

New HIPAA/HITECH Rules Bring Few Surprises, but Still Call for Sweeping Changes in Compliance Programs

More than two-and-a-half years after issuing proposed regulations under the Health Information Technology for Economical and Clinical Health (HITECH) Act, on January 17, 2013, HHS released a series of final changes to its Privacy, Security, Breach Notification and Enforcement Rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA). While the agency also supports changes required by the Genetic Information Nondiscrimination Act (GINA), the long-awaited final rules show little change over its proposals, other than a notable update to the Breach Notification Rule.

Specifically, as predicted by many in the privacy community, the agency restructured the Breach Notification Rule's rather subjective "harm threshold" used for determining when a breach occurs and notification is required. Under the final rule, most unauthorized acquisitions, accesses, uses or disclosures of protected health information (PHI) are presumed to be breaches, save a few narrow exceptions. To avoid making notifications, covered entities must now "demonstrate that there is a low probability that the protected health information has been compromised" using at least four specified factors that the agency characterizes as more "objective."

In addition to increased civil monetary penalties, perhaps the most impactful change to the HIPAA rules continues to be the extension of regulatory authority, including enforcement, to those who provide services to covered entities involving the disclosure or use of PHI, known as "business associates." Moreover, the types of entities that are considered business associates have also been expanded to include subcontractors of traditional business associates and other groups such as patient safety and health information organizations.

Other key areas of change include restrictions on marketing communications without patient authorization, particularly where the covered entity receives remuneration for the messages; strict limits on the sale of PHI without patient authorization; the exclusion of data regarding those deceased for more than 50 years from the definition of PHI; support for simplified approaches to patient involvement in research studies through the use of compound authorizations; relief for parents who wish to permit covered entities to communicate with their children's schools regarding immunizations; restrictions on using or disclosing genetic information for underwriting purposes; and patient access to data in electronic forms. Patient rights are also enhanced by requiring covered entities to honor patient requests that information regarding services paid for out-of-pocket not be shared with health plans.

HHS also provided clarification to covered entities regarding the demographic information that may be used in fundraising activities without patient authorization, such as details regarding particular treatments and outcomes. Although, patients must be given an opportunity to opt-out of such contacts. And, the final rules make it clear that covered

entities will need to update and reissue their Notices of Privacy Practices to reflect changes in patient rights and covered entity duties, including breach notification.

The effective date for the final rules is set for March 26, with compliance required by September 23, 2013. HHS has also set 180 days as the norm for compliance with HIPAA Rule changes on a going forward basis, barring special circumstances. However, the agency has provided a transition period stretching to September 22, 2014, under certain circumstances, for updating some business associate agreements.

Many covered entities and business associates may have begun planning or even implementing changes based on the proposed rules, but compliance with the new rules still requires careful analysis and significant expenditures. HHS' own estimate for first year compliance ranges from $114M to $225.4M nationwide, with $14.5M in estimated expenditures on a continuing annual basis. Important steps for covered entities and business associates (and their subcontractors) to take now include:

- Reworking breach response plans;
- Inventorying and reviewing all business associate relationships and current agreements for compliance;
- For business associates, reviewing Security Rule compliance programs; and
- For covered entities, making updates to and planning distribution of their Notices of Privacy Practices; reviewing current and planned marketing and fundraising communications programs; and reworking policies, processes and procedures in areas of change.