HIGHLIGHTS OF THE OMNIBUS HIPAA/HITECH FINAL RULE

IHS Partnership Conference
Denver, Colorado

August 2013

OVERVIEW

- On January 25, 2013, the Office of Civil Rights (OCR) of the Department of Health & Human Services (HHS) published the long-awaited omnibus final regulation governing health data privacy, security and enforcement (Omnibus Rule).

Business Associates

- The Omnibus Rule expands HIPAA's coverage to directly regulate business associates and other "downstream" entities. Compliance with the new regulations is required by September 23, 2013. For business associate agreements (BA agreements) that were in effect prior to January 25, 2013, covered entities have until September 23, 2014 to amend those BA agreements to comply with the new rules.

Business Associates

- The Omnibus Rule Expands the Definition of Business Associate
- The Omnibus Rule Directly Regulates Business Associates and Their Subcontractors
- Portions of the Privacy and Security Rules Now Apply Directly to Business Associates
- Requirement That Business Associates Enter into Agreements with Their Subcontractors

Compliance

- Certainly, covered entities and business associates will need to address the significant changes to the regulation of business associates in the Omnibus Rule. In regard to revising BA agreements, covered entities that had BA agreements in place prior to January 25, 2013 will have until September 23, 2014 to amend those agreements to comply with the new rules. To assist with this undertaking, HHS recently published sample business associate provisions, which can be http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. Aside from reviewing BA agreements, it is imperative business associates and subcontractors begin to immediately review their privacy and security policies and develop rigorous programs to comply with the Omnibus Rule as enforcement against business associates will begin in September 2013.

Breach Notification

- **Omnibus Rule Revises Definition of Breach by Adding Presumption of Breach**
- **Omnibus Rule Removes "Harm Standard" and Modifies Risk Assessment**

Marketing and Fundraising

- **Marketing**
- **Fundraising**

New Requirements for Notices of Privacy Practices

- A new NPP is required by September 2013.

Individual Rights

- **Restrictions on Uses and Disclosures of PHI**
- **Request for Access to PHI**

The Enforcement Rule

- Investigations and Compliance Reviews
- Business Associates
- Civil Monetary Penalties

• If the covered entity or business associate did not know of the violation and would not have known of the violation by exercising reasonable diligence, the penalties are no less than $100 and no more than $50,000 per violation, with an annual cap of $1,500,000 for identical violations.

• If the HIPAA violation is due to reasonable cause and not to willful neglect, the penalties are no less than $1,000 and no more than $50,000 per violation, with an annual cap of $1,500,000 for identical violations.

• If the HIPAA violation is due to willful neglect, but was corrected within 30 days of the covered entity or business associate discovering the violation, the penalties are no less than $10,000 and no more than $50,000 per violation, with an annual cap of $1,500,000 for identical violations.

• If the HIPAA violation was due to willful neglect and was not corrected within 30 days, the penalties are no less than $50,000 per violation, with an annual cap of $1,500,000 for identical violations.

The Enforcement Rule

- **Factors Considered in Determining the Amount of a Civil Monetary Penalty**
- **Affirmative Defenses**

Impact

- The Omnibus Rule significantly strengthens HIPAA enforcement, which should be of concern to all covered entities and particularly to business associates. Over the last two years OCR has become much more aggressive in enforcing HIPAA and now has a more robust enforcement rule at its disposal. Thus, it is more important than ever for covered entities and business associates to understand their obligations under HIPAA and have compliance programs in place to help make sure those obligations are met.

QUESTION???