

## **HIPAA UPDATE FINAL OMNIBUS RULE**

**Published January 25, 2013**

**Effective March 26, 2013**

**Compliance Date September 23, 2013**

### **OVERVIEW**

#### **SECURITY:**

- **Added “and business associates” with defined covered entities**
- **Defines electronic media**
- **Requires an annual review of risk assessments**

#### **PRIVACY:**

- **Business Associates added responsibility and accountability**
- **Deceased individuals: disclosures to persons involved in care or payment**
- **Childhood Immunizations: disclose to schools without signed authorization where required by state law for student admission, all other disclosures still require authorization**
- **Marketing – when authorization to disclose is required or not**
- **Fundraising: categories of PHI that may be released, opt-out opportunities, not used as condition for treatment or services**
- **Disclosure and sale of health information: requires patient authorization, authorization must specify whether or not re-disclosure is permitted**
- **Research – Clarifies compound authorizations, future use, and disclosure**
- **Requested Restrictions – restrictions from disclosure for patients who pay for services “out of pocket”**
- **Electronic Access – requires release of information in electronic format, via email, or via electronic transmission to a third party when requested by patient with a time limit of 30 days for access**
- **GINA – protections relating to genetic information and nondiscrimination**
- **Notice of Privacy Practices – requires updating and redistribution: no need to hand out to current patients, must make available (“how to obtain” is acceptable), email distribution is acceptable, notice must posted in a clear and prominent location, should be made available to all patients and distributed in the next annual mailing if applicable.**
- **Breach Notification – replaces “harm to individual” with more objective measure of compromise to the data as a threshold for breach notification**

#### **ENFORCEMENT:**

- **Adopts increased CMP (Civil Monetary Penalty) amounts and tiered levels of culpability from 2009**
- **Clarifies “reasonable cause” tier – required state of mind for the lowest tier (covered entity did not know, and in the exercise of due diligence**

would not have known of the violation) and for the highest two tiers are unchanged under Final Rule

- **Intentional wrongful disclosures may be subject to civil, rather than criminal, penalties**
- **Investigation and Resolution of Violations – requirement of Final Rule that HHS will investigate a possible HIPAA violation if a preliminary review of information from an independent inquiry by HHS indicates the possibility of willful neglect. The investigation may proceed directly to an enforcement action, particularly but not only, in the case of willful neglect.**

**However, Final Rule offers assurance that absent indications of willful neglect, HHS still will seek compliance through informal, voluntary actions in appropriate cases.**