The American Recovery and Reinvestment Act of 2009 (Stimulus bill)

Summary

Governance/Funding: The stimulus bill -

- Establishes Regional privacy education officers under HHS, National Coordinator for Health Information Technology, Federal Health Information Technology Strategic Plan, HIT Policy and Standards Committees, Chief Privacy Officer
- Allows for grants for Health Care Information Enterprise Integration Research Centers
- Establishes funding to strengthen HIT infrastructure (HHS, CDC, IHS, public health depts., etc.), telemedicine, assist providers in adoption of EHRs & electronic exchange
- Establishes HIT Regional Extension Centers – must be non-profit (up to 50% government financial assistance), focus on best practices
- Establishes grants to states for HIT planning & promotion – requires graduated matching funds
- Integrates HIT into clinical education, expands health informatics education programs
- Guidance on "minimum necessary" disclosures for exchange of information (within 18 months), HIT standards specification & adoption (testing done by NIST), guidance on de-identifying PHI (within 12 months)
- Allows creation of reimbursement incentives for improving health care quality

Practice: The stimulus bill -

- Specifies that HIPAA privacy/security laws that previously only applied to "covered entities" now also apply to "business associates" and must be incorporated into BA agreements
- Specifies that criminal and civil/monetary penalties apply to everyone, not just covered entities
- Mandates use of a certified EHR for each person in the US by 2014
- Mandates data encryption for healthcare data (standardized)
- Requires patient consent for sharing of information, even if for treatment or payment or operations
- Provides for periodic audits of entities (including BA)by HHS to verify compliance, with reviews/outcomes being made public (via HHS website) annually
- Patient has right to receive details of all disclosures of PHI going back 3 years from date of request, beginning 1/1/2011
- Prohibits sale (directly or indirectly) or remuneration for exchange of health records without patient's consent, extends to business associate – kills "data mining"
- For security breaches involving < 500 people, entity must notify each individual whose information was compromised within 60 days of discovery – burden of proof of notification, log & report annually to HHS secretary
- For security breaches involving > 500 people, entity must notify local news media within 60 days, HHS secretary immediately, law enforcement as appropriate – HHS reports breaches to congress and on website
- "Healthcare operations" excludes marketing & paid communications