HIPAA Privacy and Security Compliance

Professional Roundtable: Advanced Issues in HIPAA Compliance

The Eighteenth National HIPAA Summit

February 5, 2010

Phyllis A. Patrick, MBA, FACHE, CHC

RISK ASSESSMENT

Health Care Compliance Group

- Formal vs. Informal
- External Threats & Internal Threats
- Evaluation of Risks to Confidentiality
  - CIA
  - Policies and Procedures
  - Security Controls
- Integration of Security RA with organization's overall Risk Analyses and Risk Management processes

RELATIONSHIPS: BUSINESS ASSOCIATES & COVERED ENTITIES

Health Care Compliance Group

- Shared Responsibility and Accountability
- Challenges and Opportunities
- Business Associate Agreement
  - Guide to managing the relationship
  - Legal Agreement
  - Comprehensive documentation of expectations
- Managing Changing Relationships
  - Communication
  - Severance of relationships and development of new relationships
  - Certification of vendors

EVALUATION of SECURITY PROGRAMS

Health Care Compliance Group

- Interpretation of the Standard
  - Administrative, Technical, Physical Safeguards; Documentation
- More than addressing Technical Safeguards
- Starts with Policy
- The “Context” – Federal and State requirements (Breach, Red Flags, SSNs, HITECH)
- Management Responsibility and Accountability

Security Rule
Evaluation Standard

Perform a periodic technical and non-technical evaluation, **based initially upon the standards and implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information**, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart." [§164.308(a)(8)]

Phyllis A. Patrick

Phyllis@aphccompliance.com

914-696-3622