Managing the Regulatory Environment

ADA's Guidelines for Practice Success™ (GPS™)

ADA Tip Sheet on Business Associates

The Office for Civil Rights describes business associates (BAs) as "companies or individuals who provide services to, or perform functions or activities on behalf of, a covered entity (CE) involving the use of individually identifiable health information." Examples of business associates generally include agents, contractors, practice management software companies that have the ability to access the practice's ePHI, businesses a covered dental practice contracts with to provide translation or interpreting services, patient contact companies, and others hired to do the work of, or for, covered entities that involves protected health information (PHI). The definition includes:

- ✓ health information organizations and e-prescribing gateways, and
- ✓ entities that store PHI
- ✓ entities that provide data transmission services (with limited exceptions)

Since a covered entity can have a contract with a business associate that has a contract with a subcontractor, subcontractors are included within the scope of the definition of a business associate. OCR can bring enforcement actions directly against business associates.

- ☐ Covered entities must have "business associate agreements" containing certain required provisions with their business associates. Business associates must have similar agreements with their subcontractors.
  - ✓ In addition, business associates must comply with many HIPAA provisions, such as the:
    - technical, administrative and physical safeguard requirements under the Security Rule
    - use or disclosure limitations expressed in its contract and those in the Privacy Rule and
  - ✓ OCR can bring enforce actions directly against BAs whether or not the BA has an agreement in place with the covered entity
  - ✓ Covered entities that delegate Privacy Rule obligations to business associates, such as providing Notices of Privacy Practices (NPP) to individuals, must ensure that the business associate agreement requires the BA to comply with the Privacy Rule

- ☐ OCR can enforce HIPAA directly against business associates for noncompliance such as:
  - impermissible uses and disclosures of PHI (including more than minimum necessary)
  - the failure to:
    - o comply with the Security Rule, including risk analysis
    - o provide breach notification to the covered entity
    - o disclose compliance documentation and PHI to HHS for compliance and enforcement
    - o make available the information the CE requires to respond to patient requests for access, amendments, and accountings of disclosures
  - ✓ Contractual liability for requirements in the business associate contract

RESOURCE: OCR's Personal Health Records and the HIPAA Privacy Rule