HIPAA Overview

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Title I Health Insurance Reform
  - Title II Administrative Simplification
    - Standards for electronic health care transactions
    - National identifiers for providers, health plans, and employers
    - Privacy protection for individually identifiable health information
  - Applies to “Covered Entity” Health Plans, Providers, and Clearinghouses engaged in electronic health care transactions
- Goal: improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread and secure use of electronic data interchange in health care

HITECH Updates to HIPAA

- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Part of the 2009 American Recovery and Reinvestment Act (ARRA)
  - Increased privacy and security protections
    - Extended HIPAA privacy and security requirements to all HIPAA business associates
    - Significantly increased privacy and security breach reporting and notification processes (California law already included most of these protections)

ACA Updates to HIPAA

- Patient Protection and Affordable Care Act (ACA)
  - Signed into law in 2010
  - In addition to health care reform, also expanded and strengthened HIPAA administrative simplification provisions
    - More frequent updates
    - New transaction standards
    - Operating rules
    - Health Plan Certification requirements
    - Higher penalties for non-compliance
  - Outlined HIPAA-like privacy and security requirements for health benefit exchanges

Business Associate Agreement (Addendum) (BAA)

- Required by the HIPAA Privacy Rule
- DHCS (as a HIPAA-covered Health Plan) establishes a BAA or similar agreement with each entity performing functions or activities which involve the use or disclosure of Protected Health Information (PHI) on its behalf
- Called an Addendum because it is attached to the main contract between DHCS and the vendor
- Example: DHCS has a contract in place with Affiliated Computer Services (ACS) to act as DHCS's Fiscal Intermediary for operation of the California Medicaid Management Information System (CA-MMIS). The contract includes a BAA.

Key Privacy and Security Requirements of BA

- Permitted and prohibited uses, disclosures and safeguards
- Incident and Breach reporting and notification responsibilities
- Documentation of disclosures
- Audit, inspection, and security review requirements
- Personnel controls (training, background screening, etc.)
- Technical controls (encryption, antivirus, patching, access controls, etc.)
- Paper controls (physical security, documentation of destruction, mailing, etc.)
- Requirements flow through to subcontractors

Other Processes to Ensure Privacy and Security

- Requirement of vendor to comply with HIPAA, ACA, and all relevant federal and state laws
- Additional detailed security requirements within the vendor contract
- State review of vendor security plans, policies, and procedures
- Periodic risk assessments by vendor