HIPA-A-B-C's for Small Providers

- Why HIPAA?
  - Healthcare industry realities:
    - need for data interoperability
    - evolution from paper to electronic data
    - economic incentives
  - Patient as a consumer:
    - increasing concern about threats to individual privacy
  - Legislative guidance:
    - inconsistent laws from 50 states
    - pressure for Federal mandates
- Likely Benefits for Practices
  - Reduces efforts in business office, registration, and managing enrollments, referrals and eligibility
  - Reduces need for IS support of interface engine and EDI communication
  - Enables fee collection at time of service
  - Enables health plan / sponsor payments within 10 days
  - Reduces associated costs of the above
- HIPAA's Covered Entities
  - Virtually all healthcare providers, including physicians, hospitals, long-term care providers, home health providers, dentists, ambulance services, etc.
  - All health care payers, including insurance companies and self-insured employers
  - All healthcare clearinghouses that process or route electronic claims

- Other Affected Parties: Business Associates

  - Non-employees who perform services for a covered entity, who have access to protected health information (PHI) - e.g., attorneys, medical transcriptionists, vendors
  - Covered entities must establish contracts with Business Associates to ensure they also meet HIPAA requirements

- Transactions and Code Sets: Compliance required by October 16, 2002 (or October 16,2003, upon obtaining federal deadline extension)

  - Lack of standardization has created industry-wide inefficiencies, unnecessarily high costs, opportunities for fraud and abuse
  - HIPAA's standardized transactions include:
    - Health claims / similar encounter info
    - Enrollment / disenrollment in a health plan
    - Eligibility for a health plan
    - Healthcare payment & remittance advice
    - Health plan premium payments
    - Health claim status
    - Referral certification & authorization
    - Health claims attachments (not finalized)
    - First report of injury (not finalized)
  - If transactions are conducted electronically, HIPAA standards must be used
  - Covered entities not required to use electronic transactions -- may still use paper instead of electronic media
  - The term "electronic transfer" represents ALL electronic methods. Includes magnetic tape, disk, CD, Internet transmissions, leased or dial-up lines, and private networks, direct data entry.

    - Entities may use a business associate to conduct a transaction
    - Standard code sets include:
        - CPT 4
        - HCPCS
        - ICD - 9 CM
        - CDT (dental)
        - NDC (drugs) (Will not be mandatory for hospitals)
        - Non-medical code sets

- Transactions and Code Sets Impact on Practices

    - Will necessitate claims process modifications
    - Local codes will be eliminated
    - Patient eligibility and referrals can be processed electronically

- Unique National Identifiers: Compliance required 24 months after effective dates of final Identifier Standards

    - Purpose is to work with standard transactions and code sets to streamline healthcare administration
    - National Provider Identifier (NPI) -- Final rule expected 2002
    - National Employer Identifier (EIN) -- Final rule published in May, 2002
        - IRS Federal Employer Identification Number (FEIN) -- 9 digits
    - National Health Plan Identifier (PLANID) -- Proposed rule expected 2002

- Privacy: Compliance required April 14, 2003

    - The Privacy Rule is intended to:

    - Protect and enhance rights of consumers by providing them
        - access to their health information
        - control over PHI uses and disclosures
    - Improve healthcare quality by restoring public trust and willingness to share information
    - Improve efficiency and effectiveness by creating uniform nationwide privacy framework
- Covers electronic, paper & oral information
- Requires contracts with business associates to protect health information
- Emphasizes "minimum necessary" access
- Standards apply to "protected health information": all individually identifiable health information in any form
    - General Rule: Protected health information may not be used or disclosed for reasons other than treatment, payment or healthcare operations without specific patient authorization
- Patients must receive written notice of provider's information practices; practice must make good faith effort to obtain acknowledgement of receipt
- Patients may inspect their own health information and obtain a copy
- Patients may request amendment to health information
- Patients may receive an accounting of disclosures for purposes other than treatment, payment, and healthcare operations
- Patients may request that uses and disclosures of health information be restricted
- Patients must be provided means to report a privacy complaint
- Providers can release PHI without authorization for treatment, payment or healthcare operations, or:
    - When required by law
    - Public health Activities
    - For victims of abuse, neglect, or domestic violence

        - Health oversight
        - Judicial proceedings
        - Specific law enforcement activities
    - Providers must obtain a written patient Authorization before releasing PHI for purposes other than Treatment, Payment, and Health Care Operations, such as:
        - Marketing
        - Medical research
        - Fund-raising
    - Authorizations generally address a specific need and circumstance or span of time
    - Authorizations are required before psychotherapy notes can be released
    - Providers must identify all Business Associates that have access to or use/disclose protected health information of patients
        - Business Associate contracts must be established to ensure that Business Associates' practices support HIPAA's requirements; sanctions must be applied for non-compliance by Business Associates
    - Providers may release patient's location, condition, or death when needed to family, friends, others involved in the care of the patient
    - Providers may make other disclosures to family and others involved when in the patient's best interest

- Security: Final Rule expected soon. Compliance required 24 months after effective date
    - Security standards apply to health plans, clearinghouses, and any health care provider that electronically maintains or transmits any individual's health information
    - Standards are technology neutral and outline 4 areas of compliance. Look to the proposed Security Rule and/or your IS support person for technical details behind these requirements:
        - Administrative procedures
            - Certification

  - Chain of Trust Agreements
  - Contingency Plan
  - Formal Mechanisms: Records
  - Info Access Control
  - Internal Audit
  - Personnel Security
  - Security Configuration
  - Security Incident Procedures
  - Security Mgmt. Process
  - Termination Procedures
  - Training

- Physical security
  - Assigned Security Responsibility
  - Media Controls
  - Physical Access Controls
  - Policy - Workstation Use
  - Secure Workstation Location
  - Security Awareness Training

- Technical security services
  - Communications/Network Controls
  - Integrity Controls
  - Message Authentication

- Technical security mechanisms

            - Access Controls
            - Audit Controls
            - Authorization Controls
            - Data Authentication (corruption)
            - Entity Authentication

    - HIPAA provides for scalable security solutions, based on the practice's assessment of its particular technical environment, business needs, and risks/rewards considerations. Solutions may include:

        - Username/Password Policies and Procedures
        - Log-on/Log-off Policies and Procedures
        - Disaster/Contingency Planning for computer systems
        - System Monitoring
        - Audit Control
        - Testing
        - Virus Protection
        - Locks, Access Controls (e.g. badges, keys)
        - Security Training
        - Personnel Termination Policies and Procedures

- Overall Impact of HIPAA on Healthcare Providers

    - Necessitates greater staff attention to health-related privacy and confidentiality

        - New privacy and security policies and procedures
        - New security mechanisms and practices
        - Modification of claims and billing systems, including new transaction formats and identifiers, and elimination of local codes
        - Training of all staff on privacy awareness, new policies and procedures,

    - and system changes
    - Ongoing monitoring for compliance of organization AND individual staff
    - Consistent application of sanctions for non-compliance
    - Thorough documentation of efforts

- 6 Phases Required To Achieve Compliance

  Awareness (general staff education on what to expect from HIPAA)

  Gap Analysis (determining gaps between current and required practices)

  Implementation Planning (setting plan, budget and timeline to meet HIPAA requirements)

  Implementation (deploying the Implementation Plan)

  Training (on new policies, procedures and systems changes and updates)

  Audit and Compliance (on-going monitoring and enforcement)

- Fundamental Steps in Compliance...

  - Read and become familiar with regulations; get help where needed
  - Set objectives and scope of overall compliance effort
  - Appoint privacy and security compliance officer
  - Take inventory of computer/information systems (including paper records); understand current transactions/code sets environment and uses
  - Take inventory of security and privacy policies and procedures
  - Identify gaps and weaknesses in office practices, policies, systems, and procedures - as they relate to HIPAA requirements
  - Determine planning priorities and formulate implementation budget
  - Begin promoting HIPAA awareness within office
  - Revise and improve existing security and privacy policies; implement new policies and procedures as needed

- Deploy new physical and technical safeguards to support policies and procedures
- Integrate and roll out new or upgraded processes and systems
- Create reporting and documentation procedures with feedback mechanism
- Implement necessary ongoing changes
- Do initial workforce training on new policies and changes, and provide for ongoing training program
- Provide process for addressing privacy/security breaches when and if they arise