Business Associate Contracts: Time Is Running Out . . .

Rebecca L. Williams, RN, JD
Partner
Davis Wright Tremaine LLP
Seattle, WA
beckywilliams@dwt.com
206-628-7769

Davis Wright Tremaine LLP

. . . Or April Angst, Again

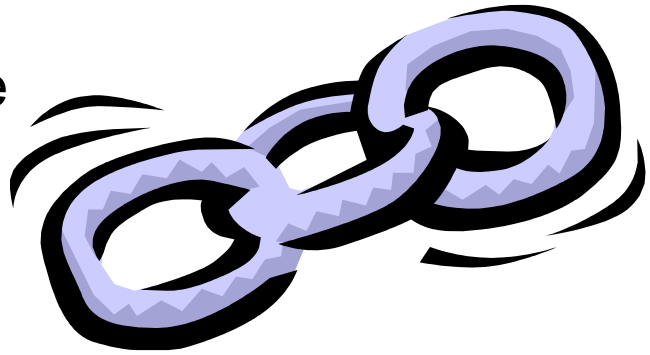
- April 2003: First deadline
- April 14, 2004: Second deadline
  - Small plans and
  - Grandfathered contracts

Two Sides to Every Contract

- Covered entity
  - Has obligation to enter into contract
  - Often want added assurances
- Business associate
  - If business associate wants to work in the industry – must contract
  - May be a covered entity
- Battle of the forms

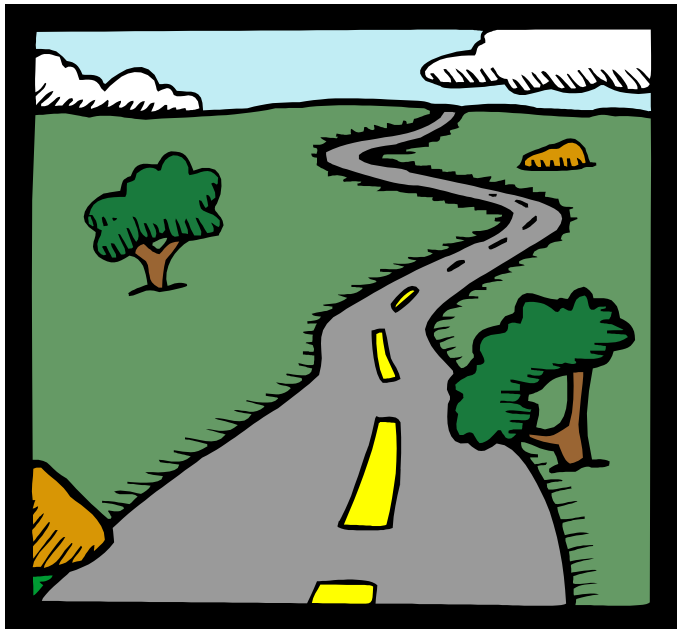
Comparison of HIPAA Contracts

- **Chain of Trust Agreement**
  - Now Eliminated in Final Security Rule
- **Trading Partner Agreement**
  - Transaction & Code Set Rule
- **Business Associate Contract**
  - Privacy and Security Rules
- **Data Use Agreement**
  - Privacy Rule (for use with limited data sets)
- **Confidentiality Agreement**
  - Long-time historical use
- Contracts may be combined as appropriate, such as
  - Clearinghouses may require Trading Partner – BAC Combo
  - BA who creates limited data sets



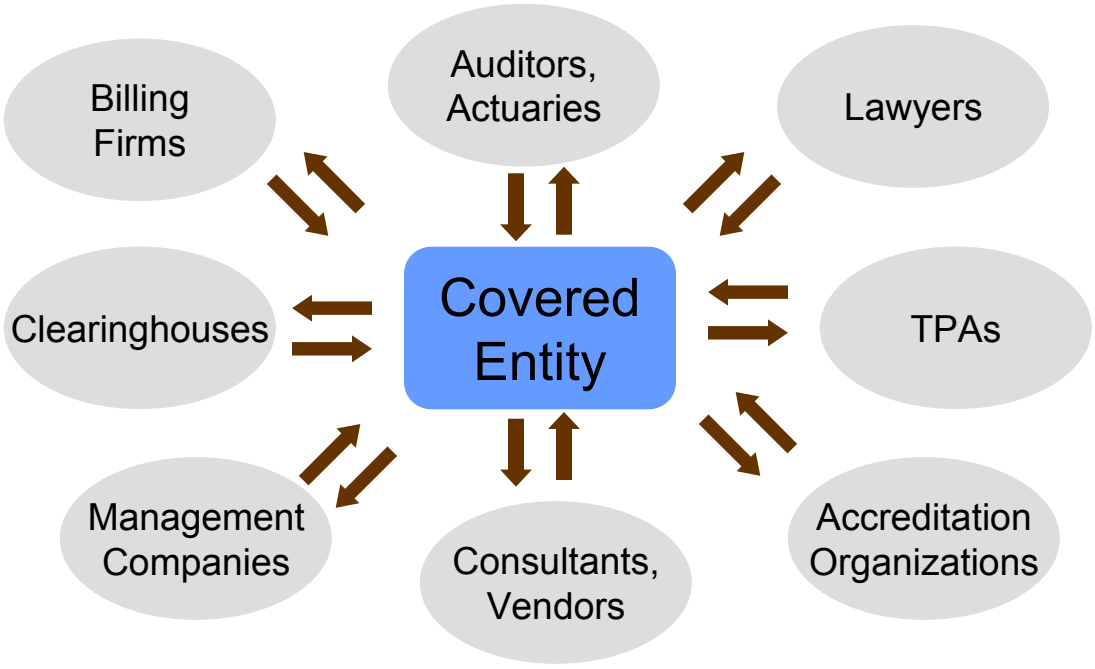
Approach to Contracting

- Contract management system
- Identification of business associate functions
- Development of templates and forms
  - How much negotiating?
  - How many forms?
  - Stand-alone contract v. addendum or exhibit
- Approval process



Need to Identify Who is a Business Associate?

- A person who, on behalf of a covered entity or OHCA —
  - Performs or assists with a function or activity involving
    - Individually identifiable information, or
    - Otherwise covered by HIPAA
  - Performs certain identified services involving PHI



Business Associate Contracts — Required Terms Under Privacy Rule

- Use and disclose information only as authorized in the contract
  - No further uses and disclosures
  - Not to exceed what the covered entity may do
- Implement appropriate safeguards
- Report unauthorized disclosures to covered entity
- Facilitate covered entity's access, amendment and accounting of disclosures obligations
- Allow HHS access to determine CE's compliance
- Return/destroy protected health information upon termination of arrangement, if feasible
  - If not feasible, extend BAC protections
- Ensure agents and subcontractors comply
- Authorize termination by covered entity

Liability . . . Of the Covered Entity

- If covered entity knows of a pattern of activity constituting a breach by the business associate, then
  - Must take reasonable steps to
    - Cure the breach or end the violation
    - Require business associate to cure
  - If unsuccessful,
    - Must terminate if feasible or
    - Report to DHHS
- How much monitoring is required?
  - Affirmative representations by business associate?
  - Investigate complaints?
- Covered entity should train its workforce to recognize and report violations by business associates

Liability . . . Of the Business Associate

- Contract Liability (e.g., damages for breach, injunctive relief)
- State privacy torts
- Criminal Liability?
  - Suggested by a U.S. Attorney's Office
  - Argue criminal provisions apply to all – not just CEs
  - Conspiracy statutes (aiding & abetting)
  - If a BA *willfully* causes an act to be done (the wrongful disclosure of PHI), which would be an offense if done by a CE, then the BA arguably could be punished as if a CE
  - Note higher standard than "knowingly"
  - Never been tested/Grain of salt

Business Associate Contracts Under Security Rule or April Angst Part III

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the
  - Confidentiality
  - Integrity and
  - Availability of *electronic* protected health information
- Ensure any agent agrees to same restrictions
- Report any "security incident"
  - Very broad
- Authorize termination if the covered entity determines business associate has breached
- When to implement?
  - Now?
  - 2005?

Limited Data Set — Not Quite De-Identified

- Limited Data Set = PHI that excludes direct identifiers except:
  - Full dates
  - Geographic detail of city, state and 5-digit zip code
- Not de-identified
- Special rules apply

Data Use Agreements

- A CE may use or disclose a limited data set for research, public health or health care operations if recipient signs data use agreement
- Required elements:
  - Establish permitted uses and disclosures by recipient
  - Establish who is permitted to use or receive limited data set
  - Require recipient to:
    - Not further use or disclose information
    - Use appropriate safeguards
    - Report impermissible use or disclosure
    - Ensure agents comply
    - Not identify the information or contact the individuals
- Beware of state law twists

Issues in Negotiations

- Covered entity obligations listed in “sample” language
  - Notice to BA
  - No nonpermissible requests
  - Obligation to notify BA of changes to NPP or PHI
- Business associate’s obligation to mitigate
  - CE has duty to mitigate under HIPAA
  - Would want assistance from BA
  - Not required

Issues in Negotiations

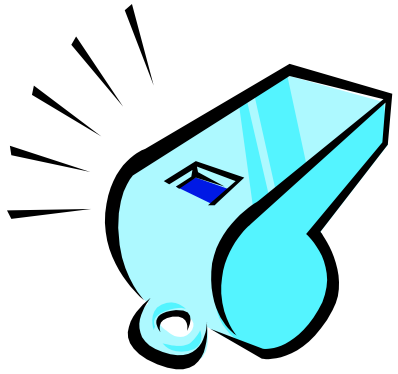
- Indemnification
- Insurance
- Limitations on liability
- Right to review contracts between business associates and their subcontractors/agents
- Right to inspect/investigate/audit
- Change in law
  - Agree to negotiate amendments
  - Unilateral amendments
  - Ability to terminate if parties do not agree to amend

Issues in Negotiations

- Termination provisions
  - Right to immediately terminate
  - Cure periods
    - Authorized to terminate
    - Not required to terminate
    - Breach of underlying contract
- Determinations of feasibility of return or destruction upon termination
  - May be built into contract

Issues in Negotiations

- What about non-applicable provisions?
- BA certifies HIPAA compliance to avoid contract
  - No go
- BA promises to comply as if it were a covered entity
- No third-party beneficiaries
  - Beneficial to both parties
- Whistleblower provision
  - 45 CFR Section 164.502(j)(1)(i)



Issues in Negotiations

- Permissible provisions
  - Allow BA to use and disclose PHI for its proper management and administration
  - Permit BA to use and disclose PHI to carry out its legal responsibilities
  - Disclosures must be required by law or with appropriate assurances
- De-identification and data aggregation (relating to CE's operations) of PHI
- Meeting state law timeframes/obligations
- Ownership of information


Questions