

# HIPAA Privacy Primer: Covered Entities, Business Associates and other HIPAA Designations

2002 Compliance Institute  
Chicago, IL

April 23, 2002

Duane Morris LLP

One Liberty Place

Philadelphia, PA 19103

Lisa W. Clark (lwclark@duanemorris.com)



# Preliminary implementation tasks

- HIPAA education
- FOCUS: DETERMINE WHAT KIND OF ENTITY YOU ARE UNDER HIPAA
- Data inventory
- Third-party inventory
- Legal documentation

# Types of organizational entities

- 1) Covered entities
- 2) Organized health care arrangement
- 3) Hybrid entities
- 4) Affiliated covered entities
- 5) Entity performing multiple covered functions
- 6) Business associates

# Privacy regulations/Covered entities

- Covered entities include:
  - Health care providers that conduct electronic transactions covered by HIPAA;
  - Health plans; and
  - Health care clearinghouses.
- Privacy regulations indirectly apply to “business associates”, i.e., persons that use PHI while performing functions or services for covered entities
  - A covered entity may be a business associate.

# Organized health care arrangement (OHCA)

- Two or more covered entities that:
  - Constitute clinically integrated setting
  - Hold themselves out as joint arrangement and participate in
    - UR activities
    - QA and QI activities; and/or
    - Payment activities, if financial risk is shared

# Hybrid entities

- HIPAA covered functions are not primary functions;
- Include health care and non-health care components
  - Some perform covered functions like a covered entity
  - Some support those performing covered functions

## Hybrid entities (continued)

- Non-health care component is responsible for compliance
- Treat different components like separate covered entities with respect to PHI
- Document designation of health care components

# Affiliated covered entities

- Legally separate entities
- Common control and ownership
- Document designation as a covered entity
- Use joint forms



# Multiple covered functions

- Perform functions that would qualify entity as combination of plan, provider and clearinghouse
- Must comply with requirements applicable to plan, provider or clearinghouse

## Business associate

A business associate is a person who performs one or more activities which involves disclosure of PHI on behalf of or for a covered entity or other entity covered by HIPAA:

- Claims processing
- Data analysis
- UR/QA
- Billing
- Benefit Management
- Practice management
- Repricing
- Professional advice
- Financial services
- Accreditation
- Any other function or activity covered by HIPAA and involving PHI.

# Business associate

Under HIPAA, a business associate is conceptually distinct from:

- Covered entity
- OHCA
- Hybrid entity
- Affiliated covered entity
- Entity performing multiple covered functions

Note: However, may be a business associate and one of these entities.

# HIPAA challenge

Which of the following is a business associate of a hospital?

- Staff physician;
- Board member;
- Wholly-owned ambulance service;
- Independent ambulance service;
- Utilization review subcontractor;
- Another hospital involved in a disease-management program;
- A physician for whom hospital bills.

# Preliminary implementation tasks

- HIPAA education
- Determine how you are designated under HIPAA
- FOCUS: DATA INVENTORY
- FOCUS: THIRD-PARTY INVENTORY
- FOCUS: LEGAL DOCUMENTATION

# Data inventory

- Data In (PHI entering entity)
- Data Out (PHI leaving entity)
- Data Within (PHI used within entity)

# Third-party inventory

- Applicable to covered entities, business associates and all other HIPAA entities
- Determine all HIPAA third-party relationships. Is third-party a:
  - Business Associate?
  - Covered Entity?
  - Other?
- Identify any other third-party that may have access to PHI

# Legal documentation/ Business associate agreements

A Business Associate Agreement is a written document that provides covered entities with “satisfactory assurances” that the business associate will “appropriately safeguard” shared PHI.



# Legal documentation/ Business associate agreements

- Develop business associate agreement language
- Develop negotiating strategy
  - Do you want to:
    - use placeholder language?
    - renegotiate entire contract?
    - enter into addendum?
  - How will costs be apportioned?

# Business associate agreements

- Permitted disclosures to third parties for:
  - Management and administrative purposes
  - Data aggregation
  - legal requirements
- Must get “reasonable assurances” from third party that PHI will be protected and notice is made of breaches

# Business associate agreements/ Limitation on uses

- Limited scope of disclosure unless required by law
- Use “appropriate safeguards” to protect PHI
- Notice of any breaches of disclosure to covered entity

# Business associate agreements/ Limitation on uses (continued)

- Limit disclosure by subcontractors and agents; “same restrictions and conditions apply” to business associate subcontractors
- How does a subcontractor differ from another third party of the Business Associate?
  - Undertakes business associate function
  - Different from a third party that supports administrative and management functions

# Business associate agreements/ Limitation on uses (continued)

- Access, amendment, and audit
  - Must “make available” PHI for these purposes
- Access by Secretary of HHS

# Business associate agreements/ Termination

- Termination by mutual breach of agreement
- Covered entity's obligation to cure material violation
- Termination/Reporting to Secretary

# Business associate agreements/ Termination

- Upon termination:
  - Destroy PHI
  - Continue agreement; or
  - Return PHI

# HIPAA Challenge

UR4U is a BA providing UR services.  
Should the contract between UR4U  
and third party address HIPAA? If so,  
how?



# HIPAA Challenge

Should, UR4U insist that the business associate agreement permit UR4U to “pass along” the PHI to a subcontractor or other third party?

# HIPAA Challenge

Should the business associate insist that the business associate agreement include a representation by the covered entity that the covered entity has obtained permission from the patient to reveal the PHI to the business associate and its subcontractors?

# HIPAA Challenge

Hospitals are asking business associates to certify that their software products are “HIPAA compliant”. What does this mean? Is it required?