HIPAA Business Associates

Second Annual HIPAA Summit
Washington, D.C.
March 1, 2001

Shana Chung
Premera Blue Cross
shana.chung@premera.com
(425) 670-4356

Paul T. Smith
Davis Wright Tremaine LLP
paulsmith@dwt.com
(415) 276-6532

Davis Wright Tremaine LLP

Premera Blue Cross
Premera Blue Cross is an Independent Licensee of the Blue Cross and Blue Shield Association

Covered Entities

- Health Plans
  - Plans that provide or pay for medical care
- Providers who transmit data electronically
  - Furnishes, bills or is paid for health care in the normal course of business
- Health Care Clearinghouses
  - Entities that process or facilitate processing non-standard data elements into standard data elements, or vice versa

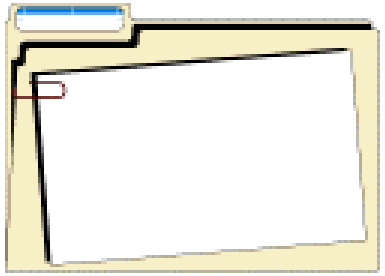
Privacy — General Rule

- A covered entity may not use or disclose Protected Health Information except:
  - pursuant to individual *consent*, for treatment, payment or health care care operations, including disclosure to business associates
  - pursuant to individual *authorization* for other specific purposes
  - without consent or authorization, for governmental and other specified purposes

Protected Health Information

"Protected Health Information"--

Individually identifiable health information transmitted or maintained in any form or medium (including oral information)

De-Identification

- Confidentiality requirements do not apply to health information that has been “de-identified”
- Qualified person must determine that risk of re-identification is “very small”
- Removal of specified identifiers creates presumption of de-identification
- CE may disclose PHI to BA for de-identification

De-Identification

Information presumed de-identified if--

The following identifiers are removed or concealed:

Name	Address	Relatives	Employer
Dates	Telephone	Fax	e-mail
SSN	MR #	Plan ID	Account #
License #	Vehicle ID	URL	IP address
Fingerprints	Photographs	Other unique identifiers	

And the CE does not have actual knowledge that the recipient could use it to identify the individual

Disclosure to Business Associates

- Must be for treatment, payment or health care operations (or it needs specific authorization)
- Requires a written agreement, except:
  - To a health care provider for treatment
  - Between group health plan and and its sponsor
  - By government health benefit programs to determine enrollment or eligibility
  - Recipient not a business associate

Disclosures Requiring Consent: Treatment

- Treatment includes--
  - Provision of health care
  - Coordination of health care
  - Referral for health care

Disclosures Requiring Consent: Payment

- Payment includes--
  - Health plan activities to determine payment responsibilities and make payment
  - Provider activities to obtain reimbursement
  - Such as--
    - coverage determinations
    - billing and claims management
    - medical review, medical data processing
    - review of services for medical necessity, coverage, appropriateness; utilization review

Disclosures Requiring Consent: Health Care Operations

- Health care operations include--
  - Quality assessment and improvement
  - Peer review, education, accreditation, certification, licensing and credentialing
  - Insurance-related activities
  - Auditing and compliance programs
  - Business planning and development
  - Business management and general administration

Minimum Necessary Information

- CE must make reasonable efforts limit uses, disclosures and requests for PHI to the minimum necessary
- Exceptions:
  - Disclosure to a provider for treatment
  - Disclosure to individual
  - Disclosure to DHHS for HIPAA compliance
  - Disclosure required by law
- Determination made by the entity
  - Balancing test

Business Associates

- Individuals and entities that receive PHI to perform or assist the performance of a function or activity on behalf of a CE
  - e.g., legal, actuarial, accounting, consulting, data aggregation, management, administrative, financial services
  - Excludes covered entity's workforce
  - Can be another covered entity

Business Associate Relationships

- CE discloses PHI to another entity who will use it on behalf of the CE
- Other entity creates PHI on behalf of the CE
- Other entity provides services to the CE, and has access to PHI

No Business Associate Relationship

- Provider and plan
- Provider and provider
- Hospital and medical staff member
- Group health plan and HMO
- PHI “conduits” (mail services and electronic equivalents)
- Financial institutions
- Due diligence activities
- Members of “organized health care arrangements”

Business Associate Contract Terms

- No use or disclosure of PHI not permitted for CE
- Safeguards to prevent unauthorized use or disclosure
- Report unauthorized disclosures to CE
- Ensure subcontractors comply with same restrictions
- Make PHI available to individuals for access and accounting
- Make records available to DHHS for compliance
- Return or destroy all PHI upon termination
- Authorize termination by CE in the event of breach
- No third-party beneficiary requirement

Business Associate Additional Uses

- Contract may permit use by business associate--
  - For management and administration of the BA
  - To carry out its legal responsibilities
- If the use involves disclosure--
  - The disclosure is required by law, or
  - The BA restricts use by person receiving disclosure, and notifies the CE of breaches

Responsibility for Business Partner's Actions

- Covered entity violates HIPAA if it —
  - "knew of a pattern of activity or practice" in violation of the agreement and
  - failed to take reasonable steps to cure the breach or terminate the contract, or report to the Secretary
- Query: How much diligence and monitoring required?

Business Partner Inventory Approach

1. Determine categories
2. Interview/survey knowledge sources
   - Interviews with the IT Contracts Department
   - Surveys to Operations/ MIP
   - Information Sessions with Functional Area Subject Matter Experts
   - Information Sessions focused on Security & Privacy
3. List & categorize partners
4. Adjust categories as necessary

Business Associate Inventory

Business Associate Information			BA Agreement		Workplan	
Category	Description	Partners	Required?	Responsibility	Actions Required	Next Steps

- 28 Detailed Categories such as
  - "Software vendors with access to PHI"
  - "Specialty Processing Groups"
- Detailed categories help ensure completeness

- 3 Basic Partner Types
  - True Business Associates who perform a function on our behalf (Processors)
  - Other Partners who don't function on our behalf but contact PHI in the natural course of providing service (Software Vendors)
  - Vendors who may have incidental PHI contact (Janitorial Services)

Partners identified to date 0385

HIPAA for the Business Associate

- Uses of PHI
  - Management and administration
  - Disclosure to contractors
- Appropriate safeguards to prevent unauthorized use or disclosure
- Accessibility
- Accountability
- Return or destruction on termination
- BA providing services for multiple CEs

HIPAA for the Business Associate

- Liability
  - Not subject to HIPAA penalties (generally)
  - Contract damages
    - Ordinary damages
    - Consequential damages
  - Indemnification

Marketing

- Disclosure permitted to a BA that assists the CE with marketing
- Communications for health-related services must--
  - Identify covered entity
  - Disclose remuneration
  - Contain opt-out (except for general newsletters)
  - If targeted based on health condition--
    - Be based on determination of benefit to patient
    - Explain why the individual has been targeted

Complex Entities

- Hybrid entities
- Affiliated covered entities
- CEs with multiple covered functions
- Organized health care arrangements
- Group health plans

Hybrid Entities

- Hybrid entity
  - covered entity whose covered functions are not its primary functions
  - covered with respect to its health care component
  - may not disclose PHI to other components, except as permitted to third parties (but it doesn't need BA agreements among its components)
  - must designate health care components

Affiliated Covered Entities

- Affiliated covered entities
  - covered entities under common ownership or control may designate themselves a single covered entity
  - If they do--
    - They may disclose PHI only as necessary for the function for which the disclosure is made
    - They would not need BA agreements

Organized Health Care Arrangements

- Clinically integrated setting involving more than one provider
- A health care system that has shared UR, QA or payment arrangements
- Group health plan and its insurer or HMO

Organized Health Care Arrangements

- Members of an OHCA--
  - Are not one another's business associates
  - May use a joint consent
  - May use a joint notice of privacy practices

Security Standards

- Require “chain of trust” agreements between business partners
- COT agreement protects integrity and confidentiality of data in EDI by maintaining the same level of protection at each link in the communication

Transaction Standards

- Anticipate a “trading partner agreement”

  Agreement specifying duties and responsibilities of parties in conducting electronic transactions