The Basics of HIPAA Business Partner and Chain of Trust Agreements

Coverage and Requirements

First National HI PAA Summit

Lisa L. Dahm, JD and Paul T. Smith, Esquire

October 16, 2000
HIPAA recognizes that health information contains personal, confidential information, and requires each health care organization to maintain the security and confidentiality of the health information within its possession.
Health Insurance Portability and Accountability Act of 1996

HI PAA

Title I
Health Insurance Portability

Title II
Administrative Simplification

Titles III, IV, V

Transaction Standards

Standard Code Sets

Unique Health Identifiers

Security Standards

Electronic Signature Standards

Info Between Health Plans

Privacy
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
All In A Name

未经授权。
Covered entities must--

- Assess potential risks and vulnerabilities to health care data
- Develop, implement and maintain appropriate security measures

Security measures must include specified requirements and features
Proposed Security Standards
General Requirements

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security for network communications
Proposed Security Standards
Administrative Procedures

- Evaluation of system & network compliance
- Chain of Trust Agreements with business partners
- Contingency plan
- Procedures for processing records
- Access control
- Internal audit of system activity
A Chain of Trust Partner Agreement is a contract entered into by two business partners in which the partners agree:

- To electronically exchange data and
- Protect the integrity and confidentiality of the data exchanged

Goal is to maintain the same level of security at each link in the chain
A Covered Entity may not use or disclose Protected Health Information except:

- for treatment, payment or health care operations, including disclosure to "business partners"
- when required by the Secretary to investigate or determine the covered entity’s compliance with the regulations
- pursuant to individual authorization
Proposed Privacy Regulations: Definitions (§ 164.504)

◆ Health Information

Any information, whether oral or recorded in any form or medium, that is:

(1) Created or received by a covered entity and

(2) Relates to the past, present, or future physical or mental health or condition of an individual, or the past, present, or future payment for the provision of health care to an individual.
Proposed Privacy Regulations: Definitions (§ 164.504) (cont’d.)

- **Individually Identifiable Health Information**
  
  Health information that is or has been electronically transmitted or electronically maintained by a covered entity which identifies the individual or from which the individual can be identified.

- **Protected Health Information**
  
  Individually identifiable information that is or has been electronically transmitted or maintained
Proposed Privacy Regulations: Definitions (§ 164.504) (cont’d.)

◆ Treatment means

- The provision of health care by health care providers
- The coordination of health care among health care providers
- The referral of a patient from one provider to another
- The coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual
Proposed Privacy Regulations: Definitions (§ 164.504) (cont’d.)

◆ Payment means

• Health plan activities to obtain premiums or to determine or fulfill responsibility for coverage and for provision of benefits under the plan

• Provider or Business Partner activities to obtain reimbursement for the provision of health care

• Activities include
  - coverage determinations
  - risk adjusting amounts
  - billing and claims management
  - review of services for medical necessity, coverage, appropriateness, or justification
  - utilization review
Proposed Privacy Regulations: Definitions (§ 164.504) (cont’d.)

◆ **Health Care Operations**

Activities undertaken by or on behalf of a covered entity for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment.

Includes:

- Quality assessment and improvement activities (outcomes evaluation and development of clinical guidelines)
- Peer and entity review, education, credentialling activities
- Insurance rating and other activities
- Conducting or arranging for medical review and auditing services (fraud and abuse detection and compliance programs)
- Compiling and analyzing information in anticipation of or for use in legal proceedings
Health Care Operations
Activities undertaken by or on behalf of a covered entity for the purpose of carrying out the management functions of such entity necessary for the support of treatment or payment.

Excludes:
- Using protected health information for marketing purposes
- Selling, renting, or bartering protected health information
- Using protected health information in a non-health related division of the same corporation
- Disclosing protected health information for purposes of making eligibility or enrollment decisions (prior to enrollment)
- Disclosing information to employers for use in making employment determinations
- Using or disclosing information for fund raising purposes
Business Partner

A person to whom the covered entity discloses protected health information so that the person can

- Carry out
- Assist with the performance of or
- Perform on behalf of

a function or activity for the covered entity

Does not include members of the covered entity’s workforce.
Business partners are contractors or other persons who receive protected health information from the covered entity:

- Lawyers, auditors, consultants
- Billing firms
- Third-party administrators (TPAs)
- Health care clearinghouses
- Data processing firms
- Private accreditation agencies
- Other covered entities
Business Partner Agreements
§ 164.506(e)

- Business Partner Agreement
  - Required for all disclosures of protected health information to a business partner
  - Exception: Disclosure by health care provider to another provider for referral or consultation
  - Covered entity contracting with the business partner must “take reasonable steps to ensure that each business partner complies with the requirements of HIPAA”
The Business Partner will:

- Not use or further disclose the information other than as permitted or required by the contract
- Not use or further disclose the information in a manner that would violate HIPAA if done by the covered entity
- Report any use or disclosure of the information not provided for by the contract of which it becomes aware
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract
- Ensure that subcontractors or agents agree to the same provisions
The Business Partner will:

- Make protected health information available to the individual who is the subject of the health information

- Make its internal practices, books and records relating to the use and disclosure of protected health information available to the Secretary

- At termination of the contract, return or destroy all protected health information received from the covered entity

- Incorporate any amendments or corrections to protected health information when notified
The Business Partner Agreement must:

- State that the individuals whose protected health information is disclosed under the contract are intended third party beneficiaries of the contract.
- Authorize the covered entity to terminate the contract if it determines that the business partner has violated a material term of the contract.

Liability for the material breach is considered to be non-compliance of the covered entity if:

- The covered entity knew or reasonably should have known of such breach and failed to take reasonable steps to cure the breach or terminate the contract.
Questions to Ponder

- What, exactly, is a health care operation?
  - Financial audit?

- Who is a business partner?
  - Subpoena/request from opposing counsel?
  - Physicians who are not employees?
  - Allied health professionals who are not employees?
  - Other covered entities?

- Can a Business Partner Agreement with a physician be modified before the end of one year? (Stark)
Questions to Ponder

- What impact will there be on current processes?
  - Marketing and fund-raising activities?
  - Disease management activities?
  - Current standard contracts and contract provisions?
  - Existing policies and procedures?
  - Costs/Benefits associated with de-identifying Protected Health Information before disclosing it?
  - Monitoring business partners and their associated agreements
    - Current review process?
    - “Evergreen” contracts?
  - Interaction with Corporate Compliance Program?
Questions to Ponder

◆ Must there be two agreements, or will one suffice?
  • Business Partner Agreement and Chain of Trust Agreement or one agreement that addresses both?

◆ What is the likely impact on the contract negotiations process?
  • Length of time required to finalize agreement?
  • Impact of the e-SIGN law?
  • Additional risk exposure to contracting parties?
Questions to Ponder

- How detailed should the Business Partner Agreement be?
  - Description of the information to be disclosed?
  - Obligations of the disclosing and receiving parties?
  - Identification and authentication procedures?
  - Permitted uses and disclosures?
  - Definition of who can view, use, disclose?
  - When/How will information be disposed of?
  - Boilerplate provisions?
  - Inclusion of security requirements?
What additional provisions (not mandated by HIPAA) should be included?

- Indemnification?
- Right of access by disclosing covered entity to books and records of business partner?
- General liability insurance coverage requirements?
- Unilateral termination by covered entity (rather than allowing business partner time to “cure”)?
- Subrogation?
- Reporting violations?
Managing Business Partner Relationships

Most Challenging Areas

- Assigning responsibility and accountability for HIPAA
- Identifying all business partners (trading, business, and chain of trust)
- Developing and administering standard contracts - Business Partner Agreements and Chain of Trust Agreements
- Drafting standard provisions
- Developing and enforcing comprehensive policies and procedures
Business Partner Agreements: What Should They Look Like Today?

- Separate from other contracts with the same Business Partner
- Until regulations are finalized, do not make patients third-party beneficiaries
- Use standard provisions wherever possible
- Include provisions to reduce risk to the covered entity:
  - Indemnification
  - Reporting violations
  - Insurance coverage
  - Unilateral termination
  - Access to Business Partner books and records and policies and procedures (assumption of risk?)
Questions
Lisa L. Dahm, J D

Senior Manager, HIPAA Advisory Services and Health Care Regulatory and Compliance Practice
Deloitte & Touche LLP, Portland, OR and Houston, TX
(503) 727-5256 and (713) 859-6700 • LDAHM@DELOITTE.COM

Relevant Experience
Ms. Dahm is a Senior Manager with Deloitte & Touche, LLP specializing in healthcare. Her experience in the healthcare industry spans more than 25 years. Prior to her graduation from law school in 1995, Ms. Dahm worked for healthcare information systems vendors, healthcare providers, and her own and another Big Five consulting firm. Before joining Deloitte & Touche, Ms. Dahm spent three years as in-house counsel for a major Integrated Delivery System located in Houston, Texas where she helped draft the System's Corporate Compliance Program, served on the Corporate Compliance Committee, responded to requests and subpoenas for business and health information, served on the System's Institutional Review Board, and advised the System on and drafted required policies, procedures, credentialing activities, and all types of contracts.

Ms. Dahm authored a monograph on patient confidentiality laws in the United States for the American Health Lawyers Association which was published in June 1999, and has written numerous articles and papers on HIPAA and other legal topics. She is a recognized expert on privacy and confidentiality, and a frequent speaker at healthcare, HIPAA, and legal regional and national conferences across the United States.

Ms. Dahm is a member of the National HIPAA Advisory Services Task Force and assisted in creating the firm's approach to providing HIPAA services to its healthcare clients. She has conducted numerous executive briefings for healthcare clients to assist them in raising awareness of HIPAA, and has managed and participated in HIPAA Privacy and other healthcare Risk Assessments. Ms. Dahm has extensive and comprehensive knowledge and understanding of healthcare laws and regulations with particular emphasis on fraud and abuse, physician transactions, Stark, and confidentiality statutes and regulations.

Ms. Dahm received her J.D. (magna cum laude) from South Texas College of Law in 1995, and was admitted to the Bar in Texas the same year.
Biography: Paul T. Smith

Paul T. Smith, Esquire
Attorney
Davis Wright Tremaine
San Francisco, California
(415) 276-6532 • PAULSMITH@DWT.COM

Relevant Experience
Paul T. Smith is a founding partner of Davis Wright Tremaine's San Francisco, California office and chair of the firm's Health Law practice group in San Francisco. He has been practicing health care and technology law in California for over 17 years. He represents hospitals, health care practitioners, medical groups and other provider organizations in corporate, transactional, financing, reimbursement and regulatory matters. He also represents software developers and web-site operators in corporate, financing, licensing and contracting matters.

Mr. Smith represents a variety of business organizations, from start-ups to established companies, particularly in the technology and health care fields. He has represented numerous start-up businesses, and he advises companies and investors in private equity and debt financing transactions, including seed financing, strategic investments, and private placements of equity and debt securities for companies at various stages of development.

Mr. Smith has represented health care providers in investigations and administrative prosecutions brought under the federal laws against kickbacks, fraud and abuse and false claims, the antitrust laws, and the prohibitions on patient dumping from emergency rooms. He has also conducted successful appeals of payment denials under the Medicare prospective payment system.

Mr. Smith also represents software developers and web-site operators in licensing, contracting and content matters.

Mr. Smith is a member of the State Bar of California, the California Society for Healthcare Attorneys, the North Bay Software and Information Technology Association, and the Silicon Valley Association of Software Entrepreneurs.

Mr. Smith received his LL.B. (cum laude) from the University of Natal in 1976 and was admitted to the Bar in California in 1980.