Business Partner Agreements

The First National HIPAA Summit
October 15-17, 2000

Paul T. Smith
Davis Wright Tremaine LLP

Health Insurance Portability & Accountability Act of 1996 (HIPAA)

- Public Law 104-191 (August 21, 1996)
- Administrative Simplification Provisions —
  - Transaction standards
  - Security standards
  - Privacy standards

Implementation

- Proposed rules
  - Issued for public comment
  - Most proposed rules already published
- Final rules
  - Transaction Standards published August 17, 2000
  - Privacy and security expected by November
- Mandatory compliance 26 months after publication of final rules

Publication Timetable

Standard	Proposed Rule Publication Date	Expected Final Rule Publication Date	Expected Compliance Date
Transactions and Code Sets	5/07/1998	8/2000 (actual)	10/2002
National Provider Identifier	5/07/1998	?	
National Employer Identifier	6/16/1998	?	
Security	8/12/1998	Fall 2000	
Privacy	11/3/1999	Fall 2000	
National Health Plan Identifier		?	
Claims Attachments		?	
National Individual Identifier	On hold	On hold	On hold

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

Transaction Standards

- Claims or encounter information
- Health plan eligibility
- Referral certification and authorization
- Health care claim status
- Enrollment and disenrollment
- Payment and remittance advice
- Premium payments
- Coordination of benefits

- First report of injury to follow

Transaction Standards

- Institutional, professional and dental transactions
  Washington Publishing Company ASC X12N standards
  www.wpc-edi.com/hipaa

- Pharmacy transactions - National Council for Prescription Drug Programs: Telecommunications Standard and Batch Transaction Standard
  www.ncpdp.org/hipaa.htm

Code Sets

Define data element values in standard transactions:

- ICD-9-CM (hospitals, ASCs)
- CPT-4 (physicians)
- HCPCS (supplies, equipment, etc.
- CDPN (dental)
- NDC (prescription drugs)

Transaction Standards: Requirements

- Providers must use standards if they conduct electronic transactions
- Health plans must--
  - use standards for electronic transactions
  - accept standard transactions, and process them promptly

Transaction Standards: Requirements

- Covered entities may use clearinghouses
- Standards apply to transactions among related entities
- Private agreements varying standards prohibited

Security Standards

- Framework for enforcing privacy standards
- Goals
  - Integrity: Protect from corruption
  - Availability: Appropriate access
  - Confidentiality: Protect from unauthorized uses or disclosures

Security Standards

- Apply to:
  - Health plans
  - Health care clearinghouses and providers that--
    - Process electronic transmissions between covered entities, or
    - Electronically maintain health information used in such a transmission

Security Standards
Basic Standard

- 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

Security Standards

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security for network communications

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

Security Standards
Administrative Procedures

- Personnel security
- Security configuration management
- Security incident procedures
- Security management processes
- Termination procedures
- Training

Chain of Trust Agreements

- Agreement between business partners to:
  - To exchange data electronically
  - Protect the integrity and confidentiality of the data exchanged
- Goal is to maintain the same level of security at each link in the chain

Security Standards
Physical Safeguards

- Assigned security responsibility
- Media controls
- Physical access controls
- Policy and guidelines on workstation use
- Secure workstation location
- Security awareness training

Security Standards
Technical Security Services

- Access control
  - Encryption is optional
- Audit controls
- Authorization control
  - Can be role-based or user-based
- Data authentication

Security Standards
Technical Security Services

- Entity authentication
  - Unique user identifier, and
  - One of the following--
    - Biometric identification
    - Password
    - PIN
    - Telephone callback
    - Token

Security Standards
Technical Security Mechanisms

- Protect data transmitted over a network--
  - Integrity controls
  - Message authentication
  - Access controls, or encryption
  - Alarm
  - Audit trail
  - Entity authentication
  - Event reporting

Privacy Standards

- Secretary of DHHS required to promulgate regulations if Congress did not act by Aug ‘99
- Proposed rules published November 3, 1999
- Comment closed February 17, 2000
  - Record # of comments received
- Final rule - September-October, 2000?

Privacy — General Rule

- A CE may not use or disclose Protected Health Information except:
  - for treatment, payment or health care care operations, including disclosure to “business partners”
  - national priority activities
  - pursuant to individual authorization

Privacy — Special Rules

- Minimum necessary disclosure
- Disclosure to business partners
- Patient rights
- Administrative procedures

Protected Health Information

- "Protected health information"--
  - Individually identifiable health information
  - that is or has been electronically maintained or transmitted by a covered entity
  - in whatever form the information exists

Protected Health Information

- Individually identifiable health information--
  - information relating to--
    - an individual's health or condition
    - provision of health care to an individual
    - payment for health care to an individual
  - identifies an individual, or there is a reasonable basis to believe it can be used to identify an individual

De-Identification

- Confidentiality requirements do not apply to health information that has been “de-identified”
- Requires removing, coding, encrypting, or otherwise eliminating or concealing, all individually identifiable information

De-Identification

- Information presumed de-identified if--
  - The following identifiers are removed or concealed:

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

  - And the CE has no reason to believe that the recipient could use it to identify the individual

Protected Health Information

- That is or has been electronically transmitted or maintained by a covered entity
  - Transmitted--key concept is whether the source or target of the transmission is a computer
  - Maintained--any electronic medium from which the information may be retrieved by a computer

Protected health information

- In whatever form the information exists
  - The standards apply to the information, not to specific records
  - Includes information in any form--electronic, written, oral
  - Also includes forms of the information existing--
    - before it was transmitted in electronic format
    - independently of the electronic record

Privacy — General Rule

- A CE may not use or disclose Protected Health Information except:
  - for treatment, payment or health care care operations, including disclosure to “business partners”
  - national priority activities
  - pursuant to individual authorization

Permitted Disclosures
Treatment

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

Permitted Disclosures 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

Permitted Disclosures
Health Care Operations

- Health care operations include--
  - Quality assessment and improvement
  - Peer review, education, accreditation, certification, licensing and credentialing
  - Insurance-related activities for individuals enrolled in an existing contract
  - Auditing and compliance programs
  - Legal proceedings

Permitted Disclosures
National Health Care Priorities

- Public health activities
- Health oversight activities
- Judicial and administrative proceedings
- Coroners and medical examiners
- Law enforcement purposes
- Governmental health data systems
- Directory purposes
- Banking and payment processes
- Research purposes, under limited circumstances
- Emergencies (to the individual or the public)
- Next of kin
- As required by other laws

Permitted Disclosures Individual Authorization

- Required elements--
  - Meaningful and specific description of information
  - Identity of persons authorized to make disclosure (may be by class)
  - Specific identity of persons to whom disclosure may be made
  - Date and signature
  - Expiration date
  - Where authorization requested by CE--
    - Description of purpose of request
    - Statement of financial gain

Privacy — General Rule

- A CE may not use or disclose Protected Health Information except:
  - for treatment, payment or health care care operations, including disclosure to “business partners”
  - national priority activities
  - pursuant to individual authorization

Permitted Disclosures Individual Authorization

- Special cases--
  - Psychotherapy notes
  - Research information unrelated to treatment
- Other rules--
  - CE may not require authorization for use or disclosure for treatment, payment or health care operations
  - CE may not condition treatment on authorization for other purposes, except for clinical trials
  - Authorization is revocable at will

Special Rules: Minimum Necessary

- CE must make “all reasonable efforts” not to use or disclose more than the minimum PHI necessary
- Exceptions:
  - Individual requests release or access
  - Disclosure to DHHS for HIPAA compliance
  - Disclosure required by law
- Determination made by the entity
  - Balancing test

Special Rules: Business Partners

- Individuals and entities that receive PHI to carry out, assist with or perform on behalf of, a function or activity for a CE
  - e.g., lawyers, auditors, consultants, TPAs, clearinghouses, data processing and billing firms, private accreditation organizations, *and other covered entities*
  - But not covered entity's workforce
- Written Assurances (business partner agreement)
  - Exception: Disclosure by health care provider to another provider for referral or consultation

Business Partner Agreement Terms

- No use or disclosure of PHI not permitted for CE
- Appropriate privacy and security safeguards
- Report unauthorized disclosures to CE
- Ensure subcontractors comply
- Make PHI available as necessary to allow individuals to exercise their right of access
- Make records available to DHHS for compliance
- Return or destroy all PHI upon termination

Responsibility for Business Partner's Actions

- Covered entity violates HIPAA if it —
  - "knew or reasonably should have known" of business partner's breach of agreement and
  - failed to take reasonable steps to cure the breach or terminate the contract
- Query: How much diligence and monitoring required?

Special Rules: Patient Rights

- Right to access, inspect, and copy PHI
- Right to written notice of information practices
- Right to request non-disclosure
- Right to request corrections and amendments
- Right to accounting of disclosures

Patient Rights
Access to PHI

- Individuals are entitled to access (inspection and copying) of their own PHI held by health plan or health care provider, including their business partners
- Exceptions--
  - Access likely to endanger life or physical safety of the individual or another
  - Information is about another, and access likely to cause substantial harm to him or her
  - Information obtained under promise of confidentiality
  - Information compiled for legal proceedings

Patient Rights
Access to PHI

- Health plans and providers required to--
  - Provide a means of request
  - Respond within 30 days
  - If the request is denied--
    - Explain why
    - Explain complaint procedures

Patient Rights
Notice of Information Practices

- Health plans and providers must provide patients with written notice of information practices
  - Uses and disclosures with and without authorization
  - Patients' rights with respect to PHI
  - Contact and complaint information
  - Must be furnished--
    - By health plans - on enrollment
    - By providers - on first service, and by posting notice

Patient Rights
Requesting Non-Disclosure

- Health care providers must permit requests
- No obligation to agree, but bound by any agreement
- Need not be imposed on business partners
- Agreement would not apply to
  - National priority activities
  - Emergency services

Patient Rights
Amendment and Correction

- Individual has right to request health plan or provider to correct PHI
- Covered entity may deny request if PHI
  - Was not created by covered entity
  - Would not be available for access to individual, or
  - Is accurate and complete

Patient Rights
Amendment and Correction

- Covered entity must have procedures for--
  - Responding to requests within 60 days
  - Implementing accepted requests
    - Includes notifying others
  - For denied requests--
    - Providing explanation and opportunity to file statement of disagreement
    - Including statement of disagreement in future disclosures

Patient Rights
Accounting of Disclosures

- Accounting includes:
  - Date of disclosure
  - Recipient name and address
  - Description of information disclosed
  - Purpose of disclosure
  - Copies of all disclosure requests
- Exceptions:
  - Treatment, payment and healthcare operations
  - Health oversight or law enforcement agencies (sometimes)

Special Rules: Administrative Procedures

- CEs must have policies, procedures, and systems to protect health information and individual rights.
  - Designation of a privacy officer and contact person
  - Privacy training for workforce
  - Administrative and technical safeguards to prevent intentional or accidental misuse of PHI
  - Means for individuals to lodge complaints
  - Sanctions for employee violations
  - Mitigation procedures

Preemption of State Law

- HIPAA preempts all "contrary" state laws
  - An entity cannot comply with the law and with HIPAA, or
  - The law is an obstacle to the purposes of HIPAA
- Exceptions--
  - State laws DHHS determines necessary for improving the health care delivery system, or address controlled substances
  - State public health laws
  - State health plan reporting laws
  - More stringent state laws

More Stringent

- State law is **more stringent** if —
  - Stricter limits on use or disclosure
  - Gives individuals greater rights of access or correction
  - Harsher penalties for unauthorized disclosure
  - Greater information to individuals regarding use or disclosure
  - Stricter requirements for authorizing disclosure
  - Stricter standards of record-keeping or accounting
  - Otherwise provides greater privacy protection

Enforcement

- CMPs against persons who fail to comply
  - $100 per violation, not to exceed $25,000/year
- Criminal penalties for knowingly disclosing or obtaining PHI or using a unique health ID
  - Knowing only: $50,000, 1 yr, or both
  - False pretenses: $100,000, 5 yrs or both
  - Use for ***commercial or personal gain*** or malicious harm: $250,000, 10 yrs or both