The Third National HIPAA Summit
October 25-26, 2001

HIPAA Privacy Manual

Keith Korenchuk
Partner, Davis Wright Tremaine LLP, Washington, D.C.

Paul Smith
Partner, Davis Wright Tremaine LLP, San Francisco

Administrative Simplification Provisions of HIPAA

- Transactions
  - Final standards effective October, 2002
- Privacy
  - Final standards effective April, 2003
- Security
  - Proposed standards published August, 1998
  - Final standards expected this year

Covered Entities

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

Privacy Rules - Status

- For delay:
  - AHA
  - Blue Cross/Blue Shield Association
  - National Organization of Governors
  - Workgroup for Electronic Data Interchange (WEDi)
- Opposed:
  - Association for Electronic Health Care Transactions (AFEHCT)

HIPAA the Law

HIPAA §1173(d)(2):

- Each [covered entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards--
  - To ensure the integrity and confidentiality of the information;
  - To protect against any reasonably anticipated--
    - threats or hazards to integrity or confidentiality, and
    - unauthorized uses or disclosures of the information;
  - Otherwise to ensure compliance by officers and employees

Privacy — General Rule

- A covered entity may not use or disclose Protected Health Information except:
  - for treatment, payment or health care care operations
    - Providers usually require a general written “consent”
  - without consent or authorization, for governmental and other specified purposes
  - pursuant to individual “authorization” for other purposes

Protected Health Information

- "Protected health information"--
  - Individually identifiable health information transmitted or maintained any any form or medium (including oral information)
  - In whatever form the information exists
    - Includes information in any form--electronic, written, oral

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”
- Qualified person must determine that risk of re-identification is “very small”
- Removal of specified identifiers creates presumption of de-identification

De-Identification

- Information is 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

Permitted Disclosures

- A covered entity may not use or disclose Protected Health Information except:
  - for treatment, payment or health care care operations
    - Providers usually require a general written “consent”
  - without consent or authorization, for governmental and other specified purposes
  - pursuant to individual “authorization” for other purposes

Required Disclosures

- To the individual, pursuant to request
- To the Secretary of DHHS, to determine compliance

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

Consent Requirements

- Required at outset of care or enrollment
- Covers treatment, payment and health care operations
- Inform patient of:
  - CE's privacy practices
  - Right to request additional restrictions
  - Right to revoke consent for future actions
- Signed and dated

Consent Requirements

- May not be combined with notice of privacy practices
- May be combined with informed consent if
  - Visually separate
  - Separately signed
- Joint consents prohibited except for organized health care arrangements that share a privacy notice

Consent Requirements

- Exceptions--
  - Indirect treatment relationship
  - Emergencies
  - Legal obligation to treat
  - Communication barriers

Disclosures Requiring Oral Agreement

- Individuals must have opportunity to agree or object to certain uses or disclosures of PHI:
  - directory (name, location, general condition & religious affiliation)
  - disclosure to family/friends involved in patient's treatment of PHI directly related to their involvement
  - notification to responsible person about location, general condition or death
- If the individual objects, CE may not disclose

Permitted Disclosures
Government and Other Purposes

- As required by other laws
- Public health activities
- Victims of abuse, etc.
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents - coroners and medical examiners
- Organ procurement
- Research purposes, under limited circumstances
- Imminent threat to health or safety (to the individual or the public)
- Specialized government function
- Workers' compensation

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

Permitted Disclosures Individual Authorization

- Other rules--
  - CE may condition treatment or enrollment on "consent"
  - CE may not condition treatment on "authorization" for other purposes, except for clinical trials
  - Authorization and consent are revocable at will, except to the extent the entity has relied on them

Research

- Disclosure of PHI created for purposes of research that includes treatment requires authorization
- Disclosure of other PHI requires authorization or "waiver" from an IRB or privacy board
- Criteria
  - No more than minimal risk to individuals
  - Research cannot be conducted without waiver
  - Risks of disclosure reasonably related to benefits
  - Adequate protection of data

Privacy — Special Rules

- Agreed restrictions
- Personal representatives
- Minors
- Psychotherapy notes

Privacy — Special Rules

- Minimum necessary disclosure
- Marketing
- Fundraising
- Business associates

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

Marketing

- No authorization required for--
  - Face-to-face encounter
  - Marketing concerning products or services of nominal value
  - Marketing concerning health-related services

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

Fundraising

- CE may use or disclose to BA or related foundation for purposes of raising funds for CE's benefit--
  - Demographic information
  - Dates of health care provided
- CE must include opt-out information in fund-raising materials

Special Rules: Organizational Requirements

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

Special Rules: Organizational Requirements

- 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

Special Rules: Organizational Requirements

- Covered entities with multiple covered functions
  - Must comply with the requirements for each function
  - May disclose PHI only as necessary for the function for which the disclosure is made
- Affiliated covered entities
  - covered entities under common ownership or control may designate themselves a single covered entity

Special Rules: Organizational Requirements

- 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

Special Rules: Organizational Requirements

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

Special Rules: Organizational Requirements

- Group health plans
  - Plan documents must restrict disclosure of PHI to sponsor by plan and insurer/HMO
  - Plan may disclose summary health information for--
    - Obtaining premium bids
    - Modifying or terminating the group health plan

Special Rules: Organizational Requirements

- Other disclosures to plan sponsor
  - Limited to plan administration functions
  - Must be pursuant to assurances relating to use and disclosure (like BA agreement)
  - No use for employment-related actions
  - “Adequate separation” between plan and sponsor

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