HIPAA

Health Privacy Rule
45 C.F.R. Part 164

August 21, 2001

HHS/OGC

- Donna Eden, Office of the General Counsel, U.S. Department of Health and Human Services
- C2-05-23, 7500 Security Blvd., Baltimore, Maryland 21244-1850
- 410.786.8859
- Donna.Eden@hhs.gov

Privacy Standards

- Congress gave itself until 1999 to enact comprehensive health privacy legislation
- On August 26, 1999, the Secretary of HHS was authorized to promulgate privacy regulations
- No standards available from ANSI accredited standards development organization

Privacy Regulations

- Notice of Proposed Rulemaking published November 3, 1999
- Final Rule published December 28, 2000
  - Effective date: February 26, 2001
  - Compliance date: February 26, 2003 or 2004
- Delay by new administration
  - New effective date of April 14, 2001
  - New compliance date of April 14, 2003 or 2004

Current status

- Office for Civil Rights delegated privacy
  - implementation
  - technical assistance
  - enforcement
- Guidance
- Modifications
- Web site for news and guidance

HIPAA Preemption

- No repeal of existing federal laws
- State laws preempted except for those:
  - determined to be necessary by the Secretary of HHS
    - » for public health, controlled substances, etc.
    - » for state health regulatory reporting
- Privacy only: No preemption for state laws if
  - contrary *and*
  - more stringent

HHS/OGC

Privacy Topics

- Protected Health Information
- New Rights for Individuals
- New Obligations for Covered Entities
- Compliance and Enforcement

Individually Identifiable Health Information

- Identifies the individual or offers a reasonable basis for identification;
- Is created or received by a covered entity or an employer; and
- Relates to past, present, or future
  - physical or mental health or condition
  - provision of health care or
  - payment for health care

HHS/OGC

Protected Health Information

- Individually identifiable health information
- Transmitted or maintained in any form by
  - a covered entity
  - its business associate
- Exceptions
  - De-identified information
  - FERPA and other specialized data

Protected Health Information (PHI)

- Individually identifiable health information
  - in any form or medium
  - not otherwise excluded, e.g., certain education and prison records
- Held by a covered entity or its business associate
- In a designated record set

New Rights for Individuals

- Receive Notice of Information Practices
- See and copy own records
- Request corrections
- Obtain accounting of disclosures
- Request restrictions and confidential communications
- File complaints

New Obligations for Covered Entities

- To use and disclose PHI only as permitted by the regulation
- To protect the integrity and security of PHI
- To ensure that business associates protect PHI
- To establish policies and implement procedures to accomplish these purposes

Covered entities may use or disclose PHI only:

- With consent, for treatment, payment or health care
- As authorized by the individual for other disclosures
- After an opportunity to agree or object
- For specific public purposes under law

Covered entities must disclose PHI:

- Upon request by the individual
- To the Office for Civil Rights for enforcement purposes
- All other releases are permissive!

What is consent?

- Agreement by patient for use of PHI for treatment, payment and operations
- Must be obtained prior to TPO
  - by direct providers
- Exceptions:
  - emergencies
  - treatment required by law
- May be obtained by plans and others

Consent Forms

- Must include:
  - Use and disclosure for TPO
  - Refer to Notice of Privacy Practices
  - Right to request restrictions
  - Right to revoke
- Individual must sign and date

What is authorization?

- Permission to covered entity to release PHI for purposes other than TPO
- Detailed, with many required elements
- Required for any releases of psychotherapy notes
- May not be required as precondition for treatment, payment, eligibility or enrollment

Consent or Authorization

- CONSENT
- General
- One time only
- Inform that PHI may be used or disclosed for TPO
- Refer to notice
- State the right to request restrictions
- If not given, treatment or enrollment *MAY BE DENIED*

- AUTHORIZATION
- Detailed
- Information to be disclosed
- Recipient of information
- Expiration date
- Right to revoke
- If not given, treatment, payment, enrollment or eligibility *MAY NOT BE DENIED*

Opportunity to agree or object

- Facility directories
- Persons accompanying patient or involved in care or payment
- Disaster relief

No consent or authorization needed for specific public purposes

- Required by law
- Public health
- Health oversight
- Research
- Law enforcement
- Investigation of abuse, neglect, violence

HHS/OGC

More Public Policy Purposes

- Decedents
- Organ procurement
- Research
- Threats to public health or safety
- Special government functions: (military, veterans, national security, international employees, correctional facilities, workers' compensation, etc.)

Required by Other Laws

- A law or regulation that compels a covered entity to disclose PHI that is enforceable in court
- Examples:
  - Public Health reporting
  - Criminal investigations

Public Health

- Public health authority
- Food and Drug Administration
- Communicable diseases
- Employer for medical surveillance of workplace for workplace illness or injury

Health Oversight

- Oversight agencies defined as “public” agencies
- To the health oversight agency, its contractors or agents
- For oversight activities authorized by law
- Exception: investigation of individual patients not considered oversight

Judicial & Administrative Actions

- Order from court or administrative tribunal
- Subpoena, request for discovery or other lawful process if satisfactory assurances of either:
  - Efforts to notify individual and offer opportunity to object or
  - Efforts to secure a qualified protective order prohibiting further use or disclosure and return or destruction of PHI

Research

- With individual authorization
- Without authorization if:
  - Waiver of authorization by privacy board or institutional review board
  - Reviews in preparation for research
  - Research on dead persons

Uses and Disclosures: Special Rules

- Marketing
- Fundraising
- Reporting by whistleblowers
- Reporting by workforce members who are victims of crime

Minimum Necessary

- Principle that only the minimum information should be used to accomplish purpose
- Not applicable to:
  - treatment
  - disclosures authorized by individual
  - standard transactions
  - disclosures required by law
  - disclosures to OCR for enforcement

Key Administrative Requirements

- Appoint Privacy Officer
- Establish administrative, technical and physical safeguards to protect PHI
- Establish & install policies & procedures for:
  - use and disclosure of PHI
  - minimum necessary determinations
  - required documentation & record retention
  - verification of persons requesting PHI

HHS/OGC

More administrative requirements

- Provide regular workforce training
- Take action against violations
- Mitigate any harmful effects of violations
- Establish mechanisms for effectuating patients' rights, including accounting and appeals
- Update policies, procedures and notices to comply with changes in law

HHS/OGC

Key Administrative Prohibitions

- Intimidate
- Discriminate
- Retaliate
- Require a waiver of rights

Organizational Issues

- Business Associates
- Hybrid Entities
- Organized Health Care Arrangements

Business Associates

- A contractor, agent or other agency that uses or has access to PHI to perform a function, activity or service for a CE, e.g.,
  - quality assurance
  - computer services
  - legal or accounting services
- Does not include disclosures between health care providers for treatment

Business Associates, continued

- CE required to obtain “satisfactory assurance” that Business Associate will protect the PHI to the same extent required of the CE
- CE is responsible for actions of its business associates
  - If knows of violation of business associate agreement and fails to act
  - BUT monitoring is not required

Hybrid Entities

- Single legal entity that has a component that is a CE, whose covered functions are not the primary purpose of the entity
- Health Care Component
  - Performs covered functions (e.g., employee clinic)
  - Other components that perform functions for component entity requiring use of PHI (e.g., accounting, data processing, scheduling)

Each Hybrid Entity Must

- Designate health care component(s)
- Ensure component complies with rules
- Ensure proper accommodations for disclosures from health care component to non-health care components

Organized Health Care Arrangements (OHCAs)

- Treated as single entity for notices and joint consents
- May include:
  - Clinically integrated care settings
  - Covered entities in joint arrangements engaging in joint activities
  - Group health plan and health insurance issuer(s) or HMO(s) with common participants
  - Group health plans under same plan sponsor

Compliance and Enforcement

- Congress established compliance schedules
- Civil penalties
- Criminal penalties for “wrongful disclosure” of IIHI and therefore PHI
- General enforcement regulation being drafted
- Privacy only: Part 160 - Subpart C

Compliance Responsibilities of Covered Entities

- Keep records and submit reports as required
- Cooperate with investigations and reviews
- Permit OCR access to facilities, books & records
- Certify and explain efforts to obtain information held by third parties if not provided

Privacy Enforcement

- Technical assistance for voluntary compliance
- Any person or organization may file complaints with OCR
- OCR may
  - investigate complaints
  - conduct compliance reviews
- OCR shall attempt to resolve noncompliance by informal means