Privacy in Health Care

Standards for Privacy of Individually Identifiable Health Information:
Final Rule

June, 2001

U.S. Department of Health and Human Services

Section 264 of HIPAA

- Call for recommendations on
  - Rights of individuals
  - Procedures for exercising those rights
  - Uses & disclosures of IIHI that should be authorized or required
- Deadlines for regs, preemption
- Consultations w/NCVHS & AG

HIPAA and Privacy

- HIPAA required the Secretary to promulgate a regulation protecting the privacy of individually identifiable health information if Congress did not enact such legislation by August 21, 1999
- Congress did not act
- The Secretary proposed a health information privacy rule on November 3, 1999

Privacy Rule Process

- NPRM published 11/3/99, >52,000 comments
- 2nd Comment period 2/28/01, plus >11,000
- Final Rule: Published 12/28/00
- Effective Date 4/14/01

  Compliance by 4/15/03

Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information in electronic transactions
  - Health plans
  - Health care clearinghouses
- Business associate relationships

Scope: What is Covered?

- Protected health information (PHI) is:
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium
- Held by covered entities or their business associates
- De-identified information is not covered

Individual's Rights

- Individuals have the right to:
  - A written notice of information practices from health plans and providers
  - Inspect and copy their PHI
  - Obtain a record of disclosures
  - Amend their medical record
  - Consent before information is released
  - Request restrictions on uses and disclosures
  - Complain about violations to the covered entity and to HHS

Key Points

- Covered entities can provide greater protections
- Required disclosures are limited to:
  - Disclosures to the individual who is the subject of information
  - Disclosures to OCR to determine compliance
- All other uses and disclosures in the Rule are permissive

Uses and Disclosures

- Must limit to what is permitted in the Rule
  - Treatment, payment, and health care operations
  - Requiring an opportunity to agree or object
  - For specific public purposes
  - All others as authorized by individual
- Requirements vary based on type

Consents for TPO

- Direct health care providers must obtain consent from an individual before using or disclosing PHI for treatment, payment, or health care operations
- Other covered entities may, but are not required to, obtain consents from individuals for these purposes
- In some cases, the covered entity may condition treatment or enrollment on the provision of an individual's consent
- Consent waived in emergency treatment and certain other circumstances

Authorizations (not TPO)

- Generally, covered entities must obtain an individual's authorization before using or disclosing PHI for purposes other than treatment, payment, or health care operations
- As a general rule, covered entities may not condition treatment, payment, or enrollment on the provision of an authorization
- Most uses or disclosures of psychotherapy notes requires authorization

Policy Exceptions

- Covered entities may use or disclose PHI without a consent or authorization only if the use or disclosure comes within one of the listed exceptions, such as
  - For uses and disclosures required by law
  - For uses and disclosures involving the individual's care or directory assistance
  - For health care oversight

Policy exceptions, con

- For research
- For law enforcement or judicial proceedings
- For public health
- For other specialized government functions
- To facilitate organ transplants

Minimum Necessary

- Covered entities must make reasonable efforts to limit the use or disclosure of PHI to minimum amount necessary to accomplish their purpose
- The rule applies minimum necessary requirements to uses, disclosures, and requests
- Does not apply to disclosures to providers for treatment
- Does not apply to uses or disclosures required by law

Business Associates

- Agents, contractors, others hired to do work of or for covered entity that requires phi
- Satisfactory assurance – usually a contract --that a business associate will safeguard the protected health information
- No business associate relationship is required for disclosures to a health care provider for treatment

Contracts or….

- Other Arrangements: MOU, regulation
- Covered entity is responsible for actions of business associates
  - If known violation of business associate agreement and failure to act
  - Monitoring is not required

Questions

- Covered entities must follow rules
- What are your relationships with covered entities?
- What are purposes of their disclosures to you?
- Or, what are the purposes of your requests for information to them?

Disclosures Could be for ….

- Health care operations
- Payment

- Health oversight
- Required by law

Relationships could be…

- Recipient of information as permitted by 164.512
- Business Associate
- Partner in an organized health care arrangement
  - Participating covered entities
  - Jointly involved in quality assessment/improvement activities re treatment, assessment by participants or third party on their behalf

Administrative Reqs

Flexible & scalable

- Covered entities required to:
  - Designate a privacy official
  - Develop policies and procedures (including receiving complaints)
  - Provide privacy training to its workforce
  - Develop a system of sanctions for employees who violate the entity's policies
  - Meet documentation requirements

Preemption

- Statute creates federal privacy floor by preemption of state law
- State law is preempted if it is contrary to the rule
- The final rule does not preempt State law if it
  - Is necessary to prevent fraud and abuse, ensure State regulation of insurance, for State reporting of health care delivery or costs, or to serve a compelling need relating to public health, safety, or welfare
  - Other public health or health plan reporting requirements
  - Is more stringent than the privacy rule

Office for Civil Rights (OCR)

- Delegation of Authority to enforce privacy rule (12/20/2000)
- Technical Assistance (TA):

  helping covered entities achieve voluntary compliance
- Investigation & resolution of complaints by HQ & regional staff
- Preemption exception determinations

Civil Monetary Penalties

- $100 per violation
- Capped at $25,000 for each calendar year for each requirement or prohibition that is violated

Criminal Penalties

- Up to $50,000 & 1 year in jail for knowingly disclosing individually identifiable health information
- Up to $100,000 & 5 years if done under false pretenses
- Up to $250,000 &10 years if intent to sell or for commercial advantage, personal gain or malicious harm
- Enforced by DOJ

Next Steps on Privacy

- April 12, 2001: Secretary announces President's decision of no delay in Rule.
- Department will issue guidance on how Rule is to be implemented and to clarify misconceptions
- Department will consider modifications to ensure quality of care and to correct unintended effects of the Rule

Clarifications/Changes

- Ensure doctors and hospitals have access to phi for treatment
- Simply consent to permit prescriptions to be filled on call-in basis
- Ensure parents have access to the medical records of their children, including mental health, substance abuse, or abortion

For More Information

OCR Privacy Website:

http://www.hhs.gov/ocr/hipaa

Toll-free Telephone Numbers:

1-866-OCR-PRIV (1-866-627-7748)

1-866-788-4989 (TTY)