Privacy in Health Care

Standards for Privacy of Individually Identifiable Health Information:
Final Rule

October, 2001

U.S. Department of Health and Human Services

Legislative History

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Subtitle F--Administrative Simplification
- Encourage development of (electronic) health information technologies (transactions)
- Easier information sharing—security and privacy

HIPAA

- Title II (Administrative Simplification) requires the promulgation of several standards, including:
  - Standards for Electronic Transactions and Code Sets
  - Security Standards
  - Electronic Signature Standards
  - National Standard Employer Identifier
  - National Standard Health Care Provider Identifier
  - National Standard Health Plan Identifier

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 (standard) electronic transactions
  - Health plans
  - Health care clearinghouses
- Business associate relationships

Standard Transactions

- Claims & Encounters
- Eligibility for a Health Plan inquiry
- Referral certification & authorizations
- Health Care Claim Status
- Health Care Payment & Remittance Advice
- Health Plan Premium Payments
- Enrollment & Disenrollment in a HP
- Coordination of Benefits

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 obtain a copy of their PHI
  - Obtain an accounting of disclosures
  - Amend their records
  - Request restrictions on uses and disclosures
  - Accommodation of reasonable communication requests
  - Complain 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 uses and disclosures involving the individual's care or directory assistance
  - For specific public purposes
  - All others as authorized by individual
- Requirements vary based on type

Consent: Rule

- Written consent required before direct treatment provider may use PHI for TPO.
- Exceptions:
  - emergency treatment situation,
  - substantial communication barriers,
  - when required by law to treat.
- Not required for:
  - Indirect Treatment Providers,
  - Health Plans,
  - Health Care Clearinghouses.

Consent: Guidance

- Phoned-in Prescriptions?
- Referral Appointments?

- HHS to propose fix regarding uses/disclosures prior to in-person contact

Consent guidance (2)

- YES,
  - Friends can pick up Prescriptions
  - Treatment consultations are ok
  - Electronic consent and signature are fine
  - Consent only needed one time
  - A chain may rely on the same consent
- NO,
  - Do not need to verify Signature
  - Revocation does not prevent billing

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 & follows its conditions;
  - Are required by law
  - Health care oversight
  - For public health

Policy exceptions, (2)

- For research
- For law enforcement
- For judicial proceedings
- For other specialized government functions
- To facilitate organ transplants
- To Coroners, medical examiners, funeral directors

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
- Most uses or disclosures of psychotherapy notes require authorization

Minimum Necessary

- Covered entities must make reasonable efforts to limit the use or disclosure of PHI to minimum amount necessary to accomplish their purpose

- Exceptions:
  - Disclosure to or request by provider for treatment
  - Disclosure to individual
  - Under authorization (unless requested by CE)
  - Required for HIPAA standard transaction
  - Required for enforcement
  - Required by law

Minimum Necessary: Rule

- “Role-based” access limits.
- Standard protocols for routine & recurring uses / disclosures.
- Review each non-routine disclosure.
- May rely on judgment of requestor if:
  - public official for permitted disclosure.
  - covered entity.
  - professional within covered entity.
  - BA for provision of professional service for CE.
  - researcher with IRB documentation.

Minimum Necessary: Guidance

- Reasonableness standard -
  - consistent with best practices in use today.
- Sign-in sheets? – Will propose fix.
- Student access? - Yes, under operations.
- Entire record? - Yes, when justified.
- Facility/process redesign? - No, only as reasonable.
- Impede care? - No.

Oral Communication: Rule

- All forms of communication covered.
- Requires reasonable efforts to prevent impermissible uses and disclosures.
- Policies and procedures to limit access/use
  - except disclosure to or request by provider for treatment purpose.

Oral Communication: Guidance

- Overheard providers? – To clarify.
- Does not require
  - Soundproof walls
  - Encrypted radio / phone calls
  - Patient access - unless recorded in designated record set.
  - Documentation, unless other reasons apply.
- New policy? - No, applied in NPRM once electronic.

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

Business Associate: Guidance

- Rule applies to BAs? - No.
  - requires CE to get assurance before giving PHI.
- CE liable for BA actions? - No.
  - liability only when CE is aware of material breach & fails to take reasonable steps to cure breach or end relationship.

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

Questions for you

- Team effort—IT, records management, medical staff, operations, legal, compliance….
- How is information shared, why, by whom?
- Sharing with contractors, others?
- Existing policies/procedures?
- Meaningful, not binder on shelf

Preemption

- Statute creates federal privacy floor by preemption of state law
- State law is preempted if it is contrary to the rule, except for certain state law that
  - 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
  - Regulates a controlled substance
  - Provides for other public health or health plan reporting
  - Is more stringent than the privacy rule

•Office for Civil Rights (OCR)

- Enforces civil rights laws
- Headquarters staff and ten regional offices
- 12/20/2000 - Delegation of Authority to enforce privacy rule

Privacy Activities (2)

- Technical Assistance (TA): helping covered entities achieve voluntary compliance
- Compliance reviews
- Investigation & resolution of complaints HQs and regional staff
- Exception determinations
- Enforcement regulation

Complaints

- Any person or organization may file complaint with OCR
- By mail or electronically
- Only for possible violations occurring after compliance date
- Complaints should be filed within 180 days
- Complaint may be filed with covered entity

Civil Monetary Penalties (CMPs)

- $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 imprisonment for knowingly disclosing IIHI
- 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

Enforcement Rule

- Not required by HIPAA
- May apply to all admin simp rules
- May address
  - compliance reviews
  - investigations
  - handling complaints
  - assessment of penalties

Privacy Now

- April 12, 2001: Secretary announces President's decision of no delay in Rule
- July 6, 2001: Department issued first general guidance
- HHS to propose modifications to ensure quality of care and to correct unintended effects of the Rule

Potential Modifications

- Workability
- “Prior consent” issues
  - Phoned-in Prescriptions
  - Referral Appointments
- Allowable Communications
- Minimum Necessary & common practices
- Potentially, appropriate access by parents to health information about their children

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)

Administrative Simplification Web Site:
http://aspe.hhs.gov/admnsimp/

How to Absorb the Rule

- On OCR website, read press release
- Review fact sheet from press release
- Read the July guidance
- Read the rule text—last 34 pages
- Finally, tackle the preamble
  - Summary
  - Topic by topic discussion & comment responses