

Privacy in Health Care

Standards for Privacy of Individually
Identifiable Health Information:
Final Rule

U.S. Department of Health and Human Services

Topics

- ◆ Individual Rights
- ◆ Uses and Disclosures
- ◆ Business Associates
- ◆ Enforcement
- ◆ To think about

Background: Privacy Provision

- ◆ Section 264
- ◆ Establishes a federal floor
- ◆ Proposed Rule issued November 3, 1999
- ◆ Over 52,000 comments received
- ◆ Final Rule published in FR December 28, 2000
 - Compliance date: February 26, 2003 (small health plans February 26, 2004)

What is Covered?

- ◆ Protected health information is:
 - Individually identifiable health information
 - Transmitted or maintained in any form or medium
- ◆ Held by covered entity or its business associate
- ◆ De-identified information is not covered

Key Points

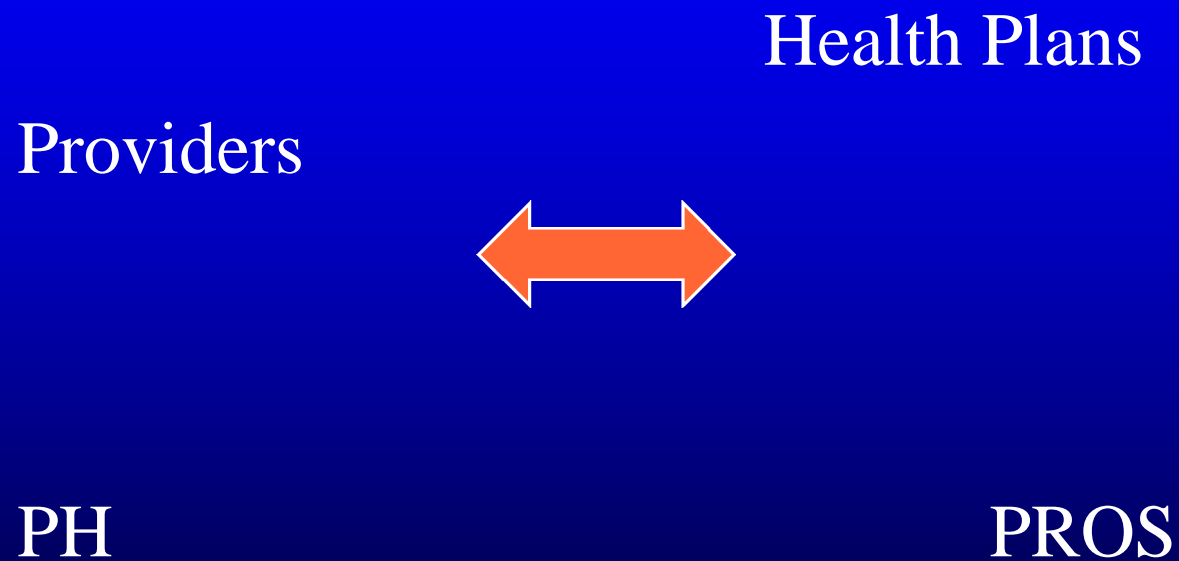
- ◆ Required disclosures are limited to:
 - Disclosures to the individual who is the subject of information
 - Compliance Disclosures to OCR
- ◆ All other uses and disclosures are permissive

Relationship to other laws

- ◆ First comprehensive health privacy protections
- ◆ Federal
- ◆ National Floor: No preemption of more protective State laws

Keep in mind...

- ◆ Rule affects disclosures & relationships



Individual Rights

- ◆ Right to inspect and copy protected health information
- ◆ Right to amend
- ◆ Right to an accounting of disclosures
- ◆ Right to have reasonable requests for confidential communications accommodated
- ◆ Right to file a complaint with OCR or with the covered entity
- ◆ Right to written notice of information practices from providers and health plans

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

Payment includes

- ◆ Utilization Review, inc precertification, concurrent & retrospective review
- ◆ Review of services re medical necessity, appropriateness of care, justification of charges
- ◆ Determinations of coverage

Health Care Operations include

- ◆ Certain quality assessment, improvement activities
- ◆ Reviewing competence of health professionals
- ◆ Accreditation, credentialing
- ◆ Medical review
- ◆ Fraud and abuse detection programs
- ◆ Certain customer service

Minimum Necessary (1)

- ◆ Restrict information to minimum amount necessary to accomplish the purpose
 - Uses: Identify types of workers, types of information, and conditions of access
 - Disclosures:
 - » Routine
 - » Non-routine
 - » Requests for disclosure
- ◆ Does not apply to disclosures to providers for treatment

Minimum Necessary (2)

- ◆ Covered entities must request minimum needed for payment review, other activities
- ◆ Providers must establish what is min nec to disclose—unless request from another covered entity
- ◆ Does not apply to disclosures required by law

Uses and Disclosures: TPO

- ◆ Treatment, payment, and health care operations
- ◆ Providers:
 - Direct treatment relationship – consent required
 - Indirect treatment relationship
 - Emergency treatment situation
- ◆ Other covered entities

What is Consent?

- ◆ One time only
- ◆ Content:
 - Inform that protected health information may be used or disclosed for treatment, payment, or health care operations
 - Refer to notice
 - State the right to request restrictions
- ◆ May condition treatment on consent
- ◆ May be revoked

Uses and Disclosures: Individual Authorization

- ◆ Permitted with an individual's authorization
- ◆ Any use or disclosure not otherwise permitted under the Rule requires authorization
 - Pre-employment physicals, employment determinations, life insurance
 - Psychotherapy notes: generally disclosure requires authorization

Uses and Disclosures: Individual Authorization

- ◆ Authorization more detailed than consent
 - Information to be disclosed
 - Recipient of information
 - Expiration date
- ◆ Must be consistent with authorization
- ◆ May not condition treatment on the individual authorizing the disclosure of information for other purposes

Uses and Disclosures: Opportunity to Agree or Object

- ◆ Facility directories
- ◆ To persons involved in care or payment for care
 - Individual's location or general condition
 - Picking up prescriptions
- ◆ Disaster relief

Uses and Disclosures: Specific Public Purposes

- ◆ Subject to various conditions:
 - As required by law
 - For public health
 - To avert serious threats to health or safety
 - For health oversight activities
 - For research
 - For law enforcement
 - Other
- ◆ Individual authorization not required

Required by law

- ◆ A mandate in law that compels a covered entity to make a use or disclosure of PHI & enforceable in court
- ◆ Ex: Medicare conditions of participation, statutes or regs that require information if payment is sought under a government program providing public benefits.

Health oversight

- ◆ To health oversight agency, its contractors or agents
- ◆ For oversight activities authorized by law, e.g., compliance with government programs
- ◆ One entity may be both a covered entity (govt health plan) and a health oversight agency

Public Health (1)

- ◆ To prevent/control disease, injury, disability...
- ◆ To report adverse events (e.g. food, dietary supplements), product defects...
- ◆ To track products
- ◆ To enable product recalls, etc

Public Health (2)

- ◆ To persons as authorized by law to notify for PH intervention or investigation
- ◆ To employers under specific circumstances for medical surveillance of workplace, work-related illness or injury

Research

- ◆ Without authorization if researcher obtains approval from IRB or “Privacy Board”
 - Privacy risks reasonable in relation to anticipated benefits,
 - plan to protect identifiers, etc
- ◆ For review to prepare a research protocol
- ◆ For research solely on PHI of decedents
- ◆ Representations re use, documentation req’d

Business Associates (1)

- ◆ Include contractors & agents
- ◆ Perform on behalf of covered entity, functions involving use/disclosure of identifiable health information
 - E.g., quality assurance, data analysis
- ◆ Perform services involving identifiable health information
 - E.g., accreditation, consulting

Business Associates (2)

- ◆ Satisfactory assurance 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

Business Associate Contracts

- ◆ Set permitted uses & disclosures
- ◆ Provide the business associate will:
 - Make no others unless required by law
 - Use appropriate safeguards
 - Report to CE any other uses/disclosures
 - At termination, return, destroy or limit further use
 - Other requirements—accounting, access, etc.

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

Enforcement (1)

- ◆ Civil monetary penalties against a covered entity which fails to comply:
 - \$100 per violation
 - Capped at \$25,000 for each calendar year for each requirement or prohibition that is violated
 - Enforcement by OCR

Enforcement (2)

- ◆ Criminal penalties for certain violations
 - Greater penalties for certain knowing violations of the Rule
 - Enforcement by the Department of Justice

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