

HIPAA Privacy Rule

Health Insurance Portability and Accountability Act of 1996
(HIPAA): *Accountability Act of 1996.*

PHS/PHP Approach

May 2002

1st HIPAA Deadline: Privacy - April 14, 2003

1996 HIPAA Statute, Title II, Subsection:
F. Administrative Simplification

Dept. Health Human
Service Regulations:



Trans-
actions &
Code Sets

Standard National Identifiers:
Provider, Employer, Payer, Individual

Security of
Health
Information

Privacy of
Health
Information

Final

Proposed

Proposed

Final

Standardize

Secure

Privacy Rule

Addresses:

- An individual's rights regarding his or her individually identifiable health information
- How to exercise those rights
- Responsibilities of organizations to support an individual's rights and,
- The use and disclosure of that information

Key Provisions

- Covered Entities
- Protected Health Information
- Business Associate Agreements
- Use and Disclosure Requirements
- New Individual Rights
- Sanctions & Penalties
- Documentation
- Workforce Training

Covered Entities

- Health care providers who transmit covered health transactions in electronic form
- Health Plans
- Health care clearinghouses

What is covered?

Protected health information (PHI)

- 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 under the Privacy Rule

PHI: Specified Identifiers

Names

All geographic subdivisions smaller than a state

street address

zip code

Telephone, Fax, E-mail addresses

Web (URL), Internet (IP) addresses

All dates directly related to an individual (except year)

DOB, admit, discharge etc.

Social Security No.

Medical Record No.

Health Plan Member No.

Full face photos

Biometric identifiers

finger or voice prints

And any unique identifier, characteristic or code that could be used alone or in combination with other information to identify an individual

Business Associates (BA)

- Entities that perform functions on behalf of PHS that involve PHI
- Satisfactory assurance through contract that BA will safeguard PHI
- PHS liability only if aware of material breach and fail to take reasonable steps to cure or end relationship

Use and Disclosure

Minimum Necessary Standard

- PHS must make reasonable efforts to limit the use/disclosure of PHI to the minimum necessary to accomplish the task

Exceptions:

- For treatment
 - Disclosure to individual who is the subject of the PHI
 - Per authorization by individual
 - Required by law
 - Required by standard transaction
 - Required by Office of Civil Rights (OCR) for enforcement
- May rely on judgement of requestor in certain situations

Use and Disclosure cont'd.

- Notice and Proposed Acknowledgement
 - Notice describes PHS/PHP use/disclosure of PHI: our policies and examples
 - Provide initially, upon enrollment or initial visit, upon revision & @3yrs
 - Providers would get acknowledgement of receipt upon first visit
- Authorization
 - Any use or disclosure not otherwise required or permitted under the Rule requires individual authorization
 - Specified purpose and timeframe
 - Cannot condition treatment/enrollment on individual signing

New Individual Rights

- Individuals have the right to:
 - A written notice of information practices
 - Control use/disclosure of their PHI
 - Authorizations & (?) Consent
 - Access / Inspect their PHI
 - Receive a copy
 - Amend (append) their PHI in designated record set

New Individual Rights cont'd.

- Individuals have the right to:
 - Request restrictions on PHI uses/disclosures
 - Have reasonable requests for confidential communications accommodated
 - Alternate means or location
 - Obtain a record of disclosures (past 6 yrs.)
 - Except: for TPO, to individual, facility directories, to persons involved in care, national security, law enforcement officers
 - Complain about violations to PHS and to DHHS

Sanctions and Penalties:

- Organizational & Individual
- Civil Monetary Penalties:
 - \$100/violation
 - \$25,000/yr cap per provision
- Criminal Penalties:
 - Knowing disclosures - 1 year /\$50,000
 - False pretenses - 5 years /\$100,000
 - Malicious or commercial intent - 10 years / \$250,000

Administrative Req's: Documentation & Training

- Designate Privacy Official
- Develop Policies & Procedures
- Provide training on Privacy P&Ps to workforce
 - All employees, volunteers, trainees, and others whose performance of work is under the direct control of PHS, whether or not they are paid.
- Develop/enforce workforce sanctions for violations
- Meet documentation requirements specified in the Privacy Rule

PHS/PHP Progress:

- Privacy Official = Jackson Ellison, CCO
- Privacy Coordinator = Debra Trout, 923-8530
- Policies/Procedure Workgroup
 - ~ 25 corporate policies
- Departmental Compliance Toolkit
 - coming in phases; starts July 2002
- All Employee Web Training - Fall 2002
- Privacy Notice will be issued
 - 1st Quarter 2003
- Building databases & documentation

What we need from you:

- Now: Tell us impact on operations
- Summer 2002:
 - Department Compliance
 - Uses & Disclosures
 - Policies and Procedures
- Fall 2002: All employee training
- Q1 2003: Collaborate on Notice