Implementation of HIPAA Requirements

Donna Eden
DHHS Office of General Counsel

- 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
- deden@os.dhhs.gov

- The information in this presentation does not represent official views of the U.S. Department of Health and Human Services

Health Insurance Portability and Accountability Act of 1996

- Established health insurance portability requirements
- Sections 261 through 263 added "Administrative Simplification" provisions to Title XI of the Social Security Act
- Section 264 added privacy provisions

HIPAA directs the Secretary of HHS to regulate:

- Standards necessary for national electronic health data systems
- Health care plans, clearinghouses and those providers who conduct designated transactions electronically
- Transmission, uses, storage and disclosure of health information

HIPAA standards:

- To be adopted from existing voluntary consensus standards, developed by ANSI approved SDO where possible
- Standards different from voluntary consensus standards may be adopted only through negotiated rulemaking
- Secretary to develop missing standards

HIPAA standards:

- Will apply to:
  - All health plans
  - All health data clearinghouses
  - Providers who conduct transactions electronically
- Will NOT apply to:
  - Employers
  - Life, casualty, disability or worker's compensation insurers
  - Other users of health information

Standards Implementation

- Numerous administrative requirements
- Compliance two (or, for small health plans, three) years following adoption
- Civil and criminal enforcement
  - By Secretary for failure to follow standards
  - By Department of Justice only for wrongful use or disclosure of information
  - No private right of action

Preemption

- HIPAA did not repeal existing federal laws
- State laws will be preempted by HIPAA standards except for laws:
  - determined to be necessary by the Secretary of HHS
  - for public health or
  - for state regulatory reporting
- Special preemption for state privacy laws

Notices of Proposed Rulemaking published summer of 1998 for:

- Transactions and Code Sets
  - Final published 65 FedReg 50312 (8/17/00)
- National Provider Identifier
- National Employer Identifier
- Security and Electronic Signatures

Transactions and Code Sets Rule

- Framework for all HIPAA requirements
- Definitions
- Place holders for preemption and enforcement
- Process for updating standards
  - Designated Standards Maintenance Organizations

Electronic Signature Standard: Update

- 1998 -- HIPAA NPRM proposed adoption of digital signature for health care
- 1999 -- Government Paperwork Elimination Act
- 2000 -- Electronic Signatures in Global and National Commerce Act

Electronic Signatures in Global and National Commerce Act

- Will give electronic documents and signatures the same legal effect as paper versions
- Consumer choice and protections
- Effective October 1, 2000
- “an electronic sound, symbol or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”

HHS/OGC

Regulations under development:

- Standard for national plan identifier
- Standard for claims attachments
- Standards for supplemental transactions
- Enforcement

Enforcement

- Civil penalties
- Criminal penalties
- Complaints to the Office for Civil Rights
- Investigations by the Office for Civil Rights

Standard on hold:

- Congress ordered work on the national individual identifier standard suspended until comprehensive privacy protections are in place
- Assorted bills before Congress to repeal the national individual identifier

Privacy Standards

- Since Congress failed to enact comprehensive federal health privacy legislation by August 26, 1999, the Secretary of HHS is required to promulgate privacy regulations to protect individually identifiable health information
- No standards available from ANSI accredited standards development organization

Individually Identifiable Health Information (IIHI)

- 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

Privacy Regulations

- Notice of Proposed Rulemaking: "Standards for Privacy of Individually Identifiable Health Information" was published November 3, 1999
- Comment period closed February 17, 2000
- Over 50,000 comments received

Key Concepts

- Floor of minimum privacy protections
- No consent required for treatment, payment or health care operations
- Business partners covered by contract
- Patients as “third party” beneficiaries
- Disclosures limited to “minimum necessary”
- Mechanism for de-identifying information
- Protections extended two years after death

Proposed regulations address:

- Obligations of plans, clearinghouses, and providers
- Rights of individuals
- Permitted uses and disclosures
  - authorized by individual
  - authorized by law or regulation
- Enforcement
- Relationship to existing laws

HHS/OGC

Affirmative obligations of plans, clearinghouse and providers:

- To ensure integrity and confidentiality of health information
  - Security
  - Administrative procedures
- To use and disclose information only as authorized
  - by subject individual
  - by law
  - by this regulation

Rights of Individuals

- Receive Notice of Information Practices
- See and copy own records
- Request corrections
- Obtain accounting of disclosures

Uses and disclosures permitted by regulation without consent:

- Public health
- Health oversight
- Law enforcement
- Research
- Judicial and administrative proceedings
- Coroners and medical examiners
- Government health data systems
- Directory services

More uses and disclosures permitted without consent:

- Banking, as necessary for payment
- Emergency circumstances
- Next-of-kin
- Otherwise required by law
- Specialized classes:
  - Military services
  - Veterans' Affairs
  - Intelligence
  - Department of State

Uses and disclosures for which consent IS required:

- Patient requested releases
- Non-health care marketing
- Fund raising
- Sale of data
- Anything not otherwise expressly
  - permitted
  - prohibited

Limited role for patients:

- No consent for most uses or disclosures
- No control over form or method of handling data
- No right to prohibit specific uses or disclosures
- No private right of action to file suit in federal court to seek relief if privacy violated

Choices

- These regulations
- Comprehensive health privacy laws
- Piecemeal fixes to existing laws
- Scott McNealy, Sun Microsystems CEO: You already have zero privacy: Get over it!

More resources

- Health Information and Technology Committee and Listserv: http://HIT@HealthLawyers.org
- For Security Forum: www.healthcaresecurity.org

And still more resources:

- For computer based record: http://www.CPRI-HOST.org
- For CPRI Toolkit http://healthcare.3com.com/securitynet/hipaa/toc.html