

# Health Information Portability and Accountability Act (HIPAA)

National Association of County  
and City Health Officials

July 2002

# HIPAA's intent



- **Improve efficiency and effectiveness of health care system by standardizing the format, content, and data elements in electronic transactions**
- **Lower the overall administrative cost of health care in the United States**
- **Protect privacy**

# HIPAA:

## Administrative Simplification

- **Transaction standards**
- **Privacy standards**
- **Security standards**
- **Other rules: national identifiers for providers, plans, employers and patients; electronic signatures; enforcement**

# Who must implement HIPAA?

**1. Health plans – Programs paying for medical care. Public plans include Medicaid, SCHIP, Indian Health Services, employee benefit plans, etc.**

**2. Health-care providers who use computers / telephones to transmit health information.**  
(examples: Case Management, chemical dependency services, assessment services, immunizations).

**3. Health Care Clearinghouses**

# Who is affected by HIPAA?

- Hospitals
- Doctor's offices
- Schools and education programs
- Jails
- Employee benefit plans
- Private and Public health plans
- **Public health and health oversight**

# **Business partner contracts**

- **Contracts must have language about transactions, and security and privacy safeguards**
- **Business partners must have security and privacy policies in place**

# HIPAA Impacts:

## State and Local governments

**Public Health**

**Social Services**

**Emergency Medical  
Services**

**Health Insurance**

**Home Health Services**

**Labor & Industries**

**Law Enforcement and  
Corrections**

**Retirement Systems**

**Medical Examiner /  
Coroner**

**Public Schools**

**NOTE: There may be others:  
Universities, Colleges, etc.**

# Reasons to be proactive

Why should you pay attention?

- **Compliance is in everyone's interest**
- **Education may help local government avoid penalties for noncompliance**
- **Noncompliance will affect local programs and services**
- **Our noncompliance will be a problem for doctors and hospitals and other business partners**

# Covered electronic transactions

- **Health-care claims**
- **Health-care payment & remittance advice**
- **Coordination of benefits**
- **Health-care claim status (*inquiry and response*)**
- **Enrollment / disenrollment in a health plan**
- **Eligibility for a health plan**
- **Health plan premium payments**
- **Referral certification and authorization**
- **Other transaction types may be added later**

# Transaction Standards

- Standardized codes and formats to conduct transactions related to health care administration and financing
- Workgroup for Electronic Data Interchange (WEDI)
- <http://www.wedi.org/>

# Privacy is a “Big Deal”

- ✓ People are alarmed by frequent media reports of privacy breaches
- ✓ Disclosure of health information can be very damaging
- ✓ There are many privacy protections in place, besides HIPAA
  - **Other Federal, State & local laws**
  - **Contractual obligations**
  - **Accreditation standards**
  - **Ethical considerations**
  - **Industry custom**

## PHI: Protected Health Information

- **Relates to a person's physical or mental health treatment....**
- **....or payment for care**
- **Identifies the individual**
- **Is created or received by a covered entity**

**Any form– electronic, paper, oral**

# **HIPAA privacy standards**

- **Individuals have specific guarantees of their privacy rights.**
- **Health care providers, plans, and business partners have new obligations.**
- **Key concepts:**
  - **Consent for treatment, payment and health care operations**
  - **Authorization for other use**
  - **Minimum necessary standard**

# General Privacy Rule

- A Covered Entity may not use/disclose PHI, except:
  - With individual “permission”
  - To the individual, upon individual’s request
  - As otherwise required (mandatory) or permitted
    - **CMS in connection with enforcement & compliance review**
    - **Other Federal law**
    - **Non-preempted State law**

## **Privacy Standards: *New Obligations***

- ✓ Designate a privacy official
- ✓ Provide privacy training to our workforce
- ✓ Develop a notice of privacy practices (listing all possible permissible disclosures made by the program) and:
  - physically post the Notice in the office
  - make a written copy available to all clients
  - update the Notice upon every material change
- ✓ Health care providers must obtain the patient's consent prior to using or disclosing protected information for treatment, payment or health care operations.

## *Security Standards: Major Components*

The proposed rule for electronic security is divided into specific categories of requirements for safeguarding data integrity, confidentiality, and availability. They are:

- ✓ Administrative Requirements
- ✓ Physical Safeguards
- ✓ Technical Security Services
- ✓ Technical Security Mechanisms

# *Unique Health Care Identifier Standards*

- ✓ *National Individual Client Identifier* – controversial, **on hold indefinitely**

Three Rules in process:

- ✓ *National Employer Identifier* – developed, to be implemented by IRS – **Final rule pending**
- ✓ *National Provider Identifier* – developed, assigned by DHHS System- **Final rule pending**
- ✓ *National Health Plan Identifier* – Still some issues, **Proposed rule pending**

## *Enforcement Standards: Future Proposed Rule*

The proposed rule for the enforcement of the HIPAA rules has not been published

All of the original proposed rules had the following penalty provision:

Civil penalties- monetary penalties at \$100 per infraction with a maximum of \$25,000 per person per year, for violation of each requirement.

## ***Enforcement Standards: Proposed Penalties***

The original privacy rule had the same provision just identified but also provided for:

Criminal penalties if the disclosure is done:-

- **Knowingly**: \$50,000, not more than 1 year prison term
- **Under false pretenses**: \$100,000, up to 5 years in prison
- **For commercial advantage/malicious harm**: \$250,000, up to 10 years in prison

# Looking ahead:

## Transactions rule

**Deadline: October 2002; extension with application to October 2003**

- **Privacy rule**

**Deadline: April 2003**

- **Security rule (anticipated)**

**Deadline (not yet set)**

# What do we need to do?

- Evaluation, planning, and compliance is similar to Y2K
- Steering Committee – representation and evaluation by ALL Agency programs and divisions
- Subcommittees – transactions, privacy, security, education
  - Representatives from effected offices / departments
- Appoint
  - Privacy Officer (Risk Management)
  - Security Officer (Technology)

# What *else* do we need to do?

- Education and awareness
- Conduct Agency-wide assessment
  - Identify risks and gaps
  - Determine “Agency-wide” vs. “Function-specific”
- Implement necessary changes
  - Policies and procedures
  - Technology
- Training and enforcement
- Audit

# HIPAA Compliance Focus

- 75 - 85% of compliance effort involves education, training, and policy formulation
- 15 - 25% of compliance effort involves technical solutions
- Approximately 80% of the risk lies within the organization

**The organization's main focus must be our employees and the best way to change / adjust their habits (procedures) and their thinking with regard to health information.**

# Details to remember:

- Privacy and security of personal health information is expected
- HIPAA is a risk management issue
- Preparation and compliance is similar to Y2K
  - Multi-year
  - Agency-wide
  - Federal requirement
- Public and private agencies effected

# Resources on the Web

- <http://pweb.netcom.com/~ottx4/HIPAA.htm>
- <http://www.hipaadvisory.com/>
- <http://www.wedi.org/>
- <http://www.hipaacomply.com/>
- <http://cms.gov/hipaa/>
- <http://fortress.wa.gov/dshs/maa/dshshipaa/>
- And there are many more...