

Health Information Portability and Accountability Act (HIPAA)

Presentation to
Board of Commissioners and
Department Directors

February 6, 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**
- **Protecting privacy**
- **Security standards**
- **Other rules: national identifiers for providers, plans, employers and patients; electronic signatures; enforcement**

HIPAA Rule Development

Administrative Simplification

The Department of Health and Human Services (DHHS) has identified five components for Implementing Title II, Subtitle F of HIPAA, Administrative Simplification:

- ✓ 1 - Electronic Standards & Code Sets
- ✓ 2 – Privacy
- ✓ 3 - Security
- ✓ 4 – Unique Health Identifiers
- ✓ 5 – Enforcement

All these rules establish national standards for the health care industry.

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: Medical Care

- **Employee Benefits Plans**
- **Private Health Insurance**
- **Medicaid**
- **Clinics, Hospitals, Physicians**
- **Other Licensed providers**

HIPAA Impacts: Social Services

- **Not traditional medical care**
- **Health related services must comply**
- **Different business models often combine provider and plan roles**
 - **Chemical Dependency**
 - **Developmental Disabilities**
 - **Mental Health**
 - **Aging and Adult Services**

HIPAA Impacts: Public Health

- **Few legal requirements but business needs will drive compliance**
- **Medicaid relationships require compliance**
- **Impacts on reporting and data release**

HIPAA Impacts: State Partners

DSHS Department of Social & Health Services

DOH Department of Health

L&I Labor & Industries

HCA Health Care Authority

DOC Department of Corrections

DRS Department of Retirement Systems

OSPI Superintendent of Public Instructions

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

Who in Thurston County?

➤ Public Health and Social Services

- Personal Health
- Environmental Health
- Mental Health
- Chemical Dependency
- Developmental Disabilities

➤ Human Resources

- Courts/Jails
- Sheriff's Office
- Medic One
- Coroner
- Area Agency on Aging

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

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

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**

Reasons to be proactive:

- 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

1. Electronic Standards

Covered Transactions

Electronic Transactions

- Health Care Claims
- Health Care Payment & Remittance Advice
- Coordination of Benefits
- Health Care Claim Status (*Inquiry and Response*)
- Enrollment and Disenrollment in a Health Plan
- Eligibility for a Health Plan
- Health Plan Premium Payments
- Referral Certification and Authorization

HIPAA Security & Privacy 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 County's main focus will be our employees and the best way to change / adjust their habits (procedures) and their thinking with regard to health information.

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
 - **DHHS in connection with enforcement & compliance review**
 - **Other Federal law**
 - **Non-preempted State law**

2. Privacy Standards

New Individual Privacy Rights

The rule provides individuals with new privacy rights to their own medical information, and includes the right to:

- ✓ Grant permission prior to the use of or the disclosure(s) of medical information
- ✓ Request a more restricted disclosure policy of their records
- ✓ Receive a written notice of privacy disclosure practices
- ✓ Obtain access to their own health care information, including the right to inspect, copy and request changes be made to their records
- ✓ Receive an accounting of all disclosures other than for treatment, payment or health care operations

2. Privacy Standards

Chain of Trust Partnership Agreements

The rule requires the use of Chain of Trust Partnership Contracts. We must establish and maintain these contracts with our business associates (e.g. contractors, vendors, service providers, auditors, etc.)

Contracts must contain provisions for cancellations, violations, and instructions on returning or destroying data at the termination of the business relationship.

Business associates with whom we share data must have comparable security and privacy policies and standards in place before the County enters into these contracts.

2. Privacy Standards

New Obligations continued

- ✓ 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.

What is HIPAA Security?

- The ability to control access & protect personal health information (PHI) from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss
- The means by which accidental, unauthorized or malicious disclosure of PHI can be avoided

Security Standards Compliance

- **Administrative Procedures**
 - **To ensure security plans, policies, procedures, training, and contractual agreements exist**
- **Physical Safeguards**
 - **To provide assigned security responsibility and controls over all media and devices**
- **Technical Security Services**
 - **To provide specific authentication, authorization, access, and audit controls to prevent improper access to electronically stored information**
- **Technical Security Mechanisms**
 - **To establish communications/network controls to avoid the risk of interception and/or alteration during electronic transmission of information**

3. Security Standards

Major Components of the Rule

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

4. Health Care Identifier Standards

Establishing Unique Health Identifiers

- ✓ 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**

5. HIPAA 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.

5. Enforcement Standards

Proposed Penalties and Costs

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

HIPAA Objectives Recap

- Reduce healthcare fraud and abuse
- Improve the efficiency and effectiveness of the healthcare system by standardizing the interchange of electronic data for administrative and financial transactions
- Protect the security and confidentiality of Protected Health Information (PHI)

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)

Reasons to be proactive:

- 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

What do we need to do?

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

What do we need to do?

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

Why do we need to do it?

- Improve security, protect privacy
- Lower costs using electronic billing
- Reduce errors
- Employee education and awareness
- Improve business partnerships

When do we need to do it?

- Appoint steering committee: March 2002
- Conduct assessment: April, May 2002
- Identify risks, gaps, compliance: June 2002
- Implement necessary changes: July – December 2002
- Training: July – December 2002 and ongoing
- Audit: January 2003 and ongoing

Details to remember:

- Privacy and security of personal health information is expected by clients, inmates, and employees
- HIPAA is a risk management issue
- Preparation and compliance is similar to Y2K
 - Multi-year
 - Potentially large cost
 - County-wide
 - Federal requirement
- Public and private agencies effected