HIPAA Privacy and Security in Local Government

Protecting Personal Data

HIPAA

The Health Insurance Portability and Accountability Act of 1996

(Kennedy/Kassabaum Act)

Case History

- Country singer Tammy Wynette's medical records were sold to the National Enquirer and Star tabloids by a hospital employee for $2,610. William Cox's position at the hospital entitled him to authorized access to several medical record databases. He retrieved medical information about Wynette and faxed it to the tabloids without her consent. Cox pleaded guilty to one count of wire fraud and was sentenced to six months in prison. ("Selling Singer's Files Gets Man Six Months," Houston Chronicle, December 2, 2000)

- The late tennis star Arthur Ashe's positive HIV status was first disclosed publicly not by himself but by a newspaper without his permission after receiving the information from a health care worker.

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet. (The Ann Arbor News, February 10, 1999)

- A banker who also served on his county's health board cross-referenced customer accounts with patient information. He called due the mortgages of anyone suffering from cancer. (M. Lavelle, "Health Plan Debate Turning to Privacy: Some Call For Safeguards on Medical Disclosure. Is a Federal Law Necessary?" The National Law Journal, May 30, 1994)

What HIPAA Does

1. Creates standards for protecting the privacy of health information
2. Protects and enhances rights of patients by providing them access and control of their information
3. Creates standards for the security of health information
4. Creates standards for electronic exchange of health information
5. Requires action as single entity
6. Mandates training for workforce members on standards and policies

Deadlines for Compliance

- Privacy
- Security
- Transactions & Code Sets
- Identifiers

- **April 14, 2003**
- **April 21, 2005**
- **October 16, 2003**
- **Fall 2004**

Privacy Rule

Covered entities may not use or disclose “Protected Health Information”, except as permitted or required by the Privacy Rule or authorized by the individual.

Protected Health Information

- Protected Health Information (PHI)
  - Identifies or can be used to identify an individual
  - Written, Spoken, or Electronic
  - Created or received by a health care provider, public health authority, employer, school or university

- Patient name
- All geographic subdivisions smaller than state
- All elements of dates related to patient
- (Date of Birth, Admission, Discharge or Death)
- Telephone numbers
- Fax numbers
- Electronic Email Addresses
- Social security numbers
- Medical record numbers
- Health plan numbers
- Account numbers
- Certificate/license numbers
- Vehicle identification and serial numbers
- Device identifiers and serial numbers
- Web Universal Resources Locators (URL)
- Internet Protocol (IP) address numbers
- Biometric Identifiers
- Full face photographs
- Any unique identifying characteristic, number, or code

PHI

Protected Health Information

Written Spoken Electronic

Release of Protected Health Information

Written patient authorization must be obtained before releasing Protected Health Information for purposes other than Treatment, Payment, and Operations

Key Components of Compliance with Privacy Rule

- Policies and Procedures
- Privacy Officer
- Training Program
- Complaint Process
- Internal compliance audit program
- Sanctions
- Incident response and corrective action procedures

Policies and Procedures

- Policy on privacy, compliance and enforcement
- Policies for use and disclosures of PHI
- Privacy policy for patients
- Administrative forms permitting disclosure
- Policies for sanctions, mitigation, and monitoring
- Policies for data security
- Policies for education and training

Covered Entities

- Health Plans
- Health Care Providers
- Health Care Clearinghouses

Employers

- Although an employer is not a covered entity, an employer must:

- Agree to comply with the rules if the employer helps to administer a health plan;

- Ensure that its health plans comply with the rules.

Health Plans

- Health Insurance
- Health HMO
- Dental
- Vision
- Health FSA
- Employee Assistance Programs
- Wellness Programs

Flexible Spending Accounts (FSA's)

- HIPAA Rules Apply to FSA's
- The Department of Health and Human Services considers Health Flexible Spending Arrangement (FSA) covered by the HIPAA privacy rules? The Department's reasoning is that a health FSA is an Employee Retirement Income Security Act of 1974 (ERISA) employee welfare benefit plan that pays for medical care. Therefore, as a health plan, it comes under the HIPAA privacy rules. Accordingly, if your employer sponsors a Health FSA it will need to review its compliance with those privacy rules. Please note that if your health FSA is self-funded, self-administered and has less than 50 participants, it is exempt from the HIPAA's privacy rules.

Health Care Provider

HIPPA defines the term "health care provider" very broadly to include any person or organization that furnishes, bills or is paid for health care in the normal course of business.

For example, local health departments, mental health area authorities, departments of social services and emergency medical services agencies may all be "health care providers" that transmit HIPAA transactions electronically. Some of these departments or agencies may serve multiple counties. In some instances, counties contract with private entities for the provision of some types of health care (such as emergency medical services).

Health Care Clearinghouse

- A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks, that does either of the following functions:
- Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
- Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Law Enforcement Agencies

- Police, firefighters and other law enforcement agencies are NOT considered covered entities under HIPAA. HIPAA does not extend, for example, to police incident reports, fire incident reports, court records, records of agencies that do not provide healthcare or insure healthcare, autopsy or any records which an individual has authorized to be disclosed.

- Fire departments that provide ambulance or emergency medical services are considered covered entities under HIPAA however, may consider themselves to be "hybrid entities" under HIPAA, and assume that no one in the department is allowed to talk to anyone, ever. If this is the case, you should approach your department about setting up procedures that allow the fire chief and/or the public information officer to get information without getting it from the people who are providing emergency medical services.

Hybrid Entity

A single legal entity that is a covered entity whose business activities include both covered and non-covered functions and that designates health care components. The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in writing. If the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care components may also include a component only to the extent that it performs covered functions or activities that would make the component a business associate of a component that performs covered functions if the two components were separate legal entities.

Enforcement Rule

On February 16, 2006, the Department of Health and Human Services issued the Final Rule regarding HIPAA enforcement. It became effective on March 16, 2006. The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations however its deterrent effects seem to be negligible with few prosecutions for violations. The Office of Civil Rights enforces this rule.

Security Rule

This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.

Goal of Security Rule

To ensure reasonable and appropriate administrative, technical, and physical safeguards that insure the integrity, availability and confidentiality of health care information

Protect against reasonably foreseeable threats to the security or integrity of the information.

Focus of Security Rule

- Both external and internal threats
- Prevention of denial of service
- Theft of private information
- Integrity of information

Security and the Privacy Rule

- Covered entities must implement appropriate technical safeguards to protect privacy of PHI.
- Covered entities must be able to reasonably safeguard against any intentional or unintentional use or disclosure that is a privacy violation.
- Covered entities should work in conjunction with “minimum necessary” rule
- Coordinated with HIPAA security regulations.

Security Rule
3 Categories

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards

Administrative Safeguards 9 Standards

1. Security Management Process
2. Assigned Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security Awareness Training
6. Security Incident Procedures
7. Contingency Plan
8. Evaluation
9. Business Associate Contracts and Other Arrangements

Physical Safeguards
4 Standards

1. Facility Access Controls
2. Workstation Use
3. Workstation Security
4. Device and Media Controls

Technical Safeguards
5 Standards

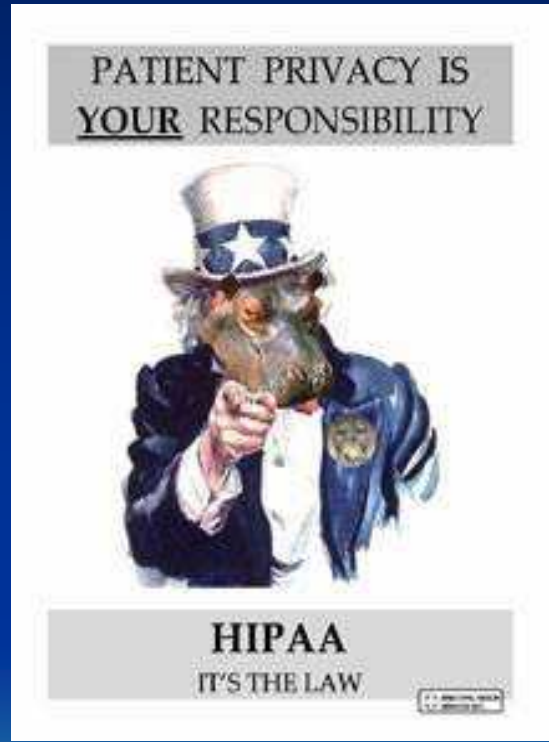
1. Access Control
2. Audit Controls
3. Integrity
4. Person or Entity Authentication
5. Transmission Security

Local Government Impact

- Significant financial implications
- High level of risk to individuals and to institution
  - civil monetary penalties
  - criminal sanctions
- Requires a change in the way we do business
  - New policies & procedures
  - Limits access to information

Penalty

The civil and criminal consequences of noncompliance or violations can be severe. Fines can reach $25,000 for multiple violations of the same standard in a calendar year, or $250,000 and/or imprisonment up to 10 years for knowingly misusing individually identifiable health information.



Next Steps

Next Steps

Determine if you are a covered entity

Identify Privacy and Security Officer

Survey areas with Electronic Protected Health Information (Human Resources, Police Department, Fire Department (EMS)

Complete a Risk Assessment

6 Phases Required to Achieve Compliance

1. Awareness (general staff education on what to expect from HIPAA)
2. GAP Analysis (determining gaps between current and required state)
3. Implementation Planningh (developing plan, budget and timeline to meet HIPAA requirements)
4. Implementation (deploying the Implementation Plan)
5. Training (on new policies, procedures and systems changes and updates)
6. Audit and Compliance (on-going monitoring and enforcement)

Fundamental Steps in Compliance...

- Read and become familiar with regulations; get help where needed
- Set objectives and scope of overall compliance effort
- Appoint privacy and security compliance officer
- Take inventory of computer/information systems (including paper records); understand current transactions/code sets environment and uses
- Take inventory of security and privacy policies and procedures
- Identify gaps and weaknesses in office practices, policies, systems, and procedures - as they relate to HIPAA requirements
- Determine planning priorities and formulate implementation budget
- Begin promoting HIPAA awareness within office
- Revise and improve existing security and privacy policies; implement new policies and procedures as needed
- Deploy new physical and technical safeguards to support policies and procedures
- Integrate and roll out new or upgraded processes and systems
- Create reporting and documentation procedures with feedback mechanism
- Implement necessary ongoing changes
- Do initial workforce training on new policies and changes, and provide for ongoing training program
- Provide process for addressing privacy/security breaches when and if they arise