

The Health Insurance Portability and Accountability Act (HIPAA)

CIS/CSE 583

Syracuse University

HIPAA

Four objectives:

- Assure health insurance portability by eliminating job-lock due to pre-existing medical conditions
- Reduce healthcare fraud and abuse
- Enforce standards for health information
- Guarantee security and privacy of health informatio

HIPAA

Title I Insurance Reform

Title II Administrative Simplification

Title III Medical Savings Accounts

Title IV Group healthcare provisions

Title V Revenue offset provisions

HIPAA

Title I ...

Title II Administrative Simplification

Title III ...

Title IV ...

Title V ...

Administrative Simplification

- Rules that the medical and insurance industries must follow in handling records, transactions, etc.
- Specific deadline dates
 - E.g., standard for electronic transactions kicked in 16 Oct 2002 (16 Oct 2003 for small health plans; except delayed by Pres. Bush for one year)

AS Areas

- Standards for Privacy of Individually Identifiable Health Information
- National Provider Identifier
- Employer Identifier
- Security and Electronic Signatures
- Standardized electronic transaction format

Note: HIPPA doesn't actually set the rules, it directs HHS to set the rules.

A Few Privacy Breaches

- A banker, also on a county health board, called in mortgages for cancer patients.
- A NYC candidate for Congress had her patient records, documenting a suicide attempt, anonymously FAXed to newspapers (she won).
- Consumer Reports found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission.

Disclosure of Medical Records

- To the patient
- To provide medical treatment (with or without consent, except psychotherapy notes) OR payment
- Under special authorization (e.g., for marketing)

Security

- Administrative procedures
- Physical safeguards
- Technical security services
- Technical security mechanisms

Administrative Procedures

Documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.

Physical Safeguards

These relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

Security Services

These include the processes that are put in place to protect and to control and monitor information access,

Security Mechanisms

These include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

Sources

- <http://aspe.hhs.gov/admnsimp/>
- <http://www.hhs.gov/ocr/hipaa/>