HIPAA: The Law

• Health Insurance Portability and Accountability Act of 1996
  • Also known as Kennedy-Kassebaum Act
• Legislation had wide regulatory impact
  • Medicare Fraud to Medical Savings Accounts.
• Department of Health and Human Services
  • Responsible for creating regulations
  • Office of Civil Rights responsible for enforcement

HIPAA - Three Relevant Parts

• Standards for electronic exchange of health information
  • Rules governing transfer of health information between organizations
• Privacy of health information
  • Rules to protect the privacy of health information
• Security of health information
  • Rules to protect against threats, hazards or unauthorized access to health information

Privacy Regulations

Current Status

• Current Regulations
  • Published December 28, 2000
  • Became effective April 14, 2001
  • Compliance required by April 14, 2003
• Proposed Modifications
  • Published March 27, 2002
  • Comment period ends April 26, 2002
  • Final regulations expected before October 14, 2002

Definitions

• Protected Health Information (PHI)
  • Individually Identifiable Health Information
  • Created or received by a health care provider, public health authority, employer, school or university
• Individually Identifiable Health Information
  • Related to an individual; the provision of health care to an individual; or payment for health care
  • and that identifies the individual
  • or a reasonable basis to believe the information can be used to identify the individual

Identifiers

• Names
• Street address, city, county, zip code
• Dates (except year) for dates related to an individual
• Telephone/Fax #’s
• E-mail, URLs, & IP #’s
• Social security numbers
• Account/Medical rec #’s
• Health plan beneficiary numbers
• Certificate/license #’s
• Vehicle id’s & serial #’s
• Device id’s & serial #’s
• Biometric identifiers
• Full face images
• Any other unique identifying number, characteristic, or code

Definitions

• Minimum Necessary:
  • Release only the minimum information necessary for the intended purpose.
• Exceptions
  • Release of information to other health care providers involved in the patient’s treatment
  • De-identified health information
Definitions

• Covered Entity
  • Health care provider who transmits any health information in electronic form in connection with HIPAA regulations.
  • Health care provider means a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

• Use
  • Sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity

• Disclosure
  • Release, transfer, provision of access to, or divulging, in any other manner, information outside the entity

Individual’s Rights

• Request restrictions on uses and disclosures of health information
• Obtain documentation of disclosures
• Inspect and copy health information
• Request amendment of health information
• File a complaint of non-compliance

Privacy Policy

• Must provide patients with a written notice of privacy policy
  • Describe and give examples of uses and disclosures of health information
  • State the individual’s rights
  • Make good faith efforts to obtain a written acknowledgment of the notice at the time of first service delivery (proposed)

Consent

• Allows for uses or disclosures to carry out treatment, payment, or health care operations
• Separate authorization required for research
• Must obtain prior to using health information
• May condition treatment on consent
• Patient may revoke consent any time
• Must document and retain signed consent for at least six years
• Would not be required under proposed rule changes

Authorization

• Usage specific consent
• Required for uses and disclosures outside of treatment, payment and health care operations
  • Research, release of records
  • Describe the usage in a “specific and meaningful fashion” and identify the person(s) using the PHI
  • Have an expiration date or event
  • Cannot coerce signature or condition treatment
  • Could have major impact on clinical research
Research use and disclosure without authorization

- Obtain waiver of authorization
- Approved by IRB or privacy board
- Similar to E4 exemption
- Preparation for research
  - May not copy or remove health information
  - Only access what is needed for research
  - Research on deceased individuals

Use and disclosure without consent or authorization

- Required by law
  - Victims of abuse, neglect, or domestic violence
- Public health activities
  - Surveillance, vital events, child abuse
  - FDA: adverse events, product tracking, post marketing surveillance
- Employers
  - Workplace medical surveillance
  - Workplace related injury or illness
  - To avert serious threat to health or safety

Disclosure Auditing

- Must maintain record of disclosure for six years
  - Including disclosures without authorization
- For each disclosure must document
  - Date
  - Name of person/entity who received PHI
  - Brief description of PHI disclosed
  - Brief statement of purpose of disclosure
- Must provide documentation within 60 days if requested by patient

Administrative Requirements

- Must designate a privacy official
- Training
  - Must train all personnel that may contact PHI
  - Must ensure staff are up to date when changes in policy are made
  - No requirement for certification/retraining
- Must have a process for complaints

Requirements for Business Associates

- Must take steps to ensure all business associates protect the privacy of health information
- Must have patient consent or authorization for business associates to use that health information
- Business associates must not violate the privacy regulations and should have a defined privacy policy
- Covered entity is accountable for business associates use or misuse of information.
- Will impact pharmaceutical and medical school joint research projects

Security Requirements

- Must adopt written security procedures
  - Who has access to health information
  - How health information will be used
  - When health information would be disclosed
- Maintain reasonable and appropriate administrative, technical, and physical safeguards
  - to ensure the integrity and confidentiality of the information
  - to protect against any reasonably anticipated
    - threats or hazards to the security or integrity of the information
    - unauthorized uses or disclosures of the information
Penalties

- Failure to comply
  - Up to $100 per violation
  - Up to $25,000 per person, per year, per standard
- Wrongful disclosure of health information
  - Improperly obtaining or disclosing health information
    - Fined up to $50,000 and/or imprisoned 1 yr
    - If under false pretenses, $100,000 and/or 5 yrs
    - If intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm: $250,000 and/or 10 yrs

Impact on Clinical Operations

- Regulations potentially impact on almost all aspects of patient care
  - Will require significant policy changes
  - Will require training of all employees
- Additional administrative requirements will slow transfer of health information
  - Minimum necessary rule
  - Auditing of disclosures
  - Major changes in workflow if consent regulation remains

Impact on Research

- Additional burden of determining and monitoring compliance with regulations
  - IRB vs. privacy board
- Need to obtain project-specific patient authorization
- Patient authorization tracking and management
- Costs and administrative time to protect all research data
- Will likely require a major redesign of how research data is stored, managed and retrieved.

Impact on Education

- Significant culture shift in the handling of patient information in training programs
  - Patient information on 3x5 cards, PDAs
  - “Teaching files” need review for PHI
  - 35mm slides, X-Rays, Lab data, video…
  - Education of medical students
    - Must be aligned with attending and resident education to achieve culture shift

Preliminary Approach

- Stanford University HIPAA Steering Committee
  - A Subcommittee of the Institutional Compliance Program
  - Membership from University, Hospitals, Medical School
- Hospital HIPAA Committee
  - Joint planning for SUMC, LPCH
  - Focus on clinical operations and patient data on hospital network
  - School is working very closely with this committee
- School of Medicine HIPAA Planning Group
  - Office of SAD for Information Resources and Technology
    - Focus on School-specific HIPAA planning and implementation
  - Our particular focus will be impact on research and education
  - Discussions with IRB on research compliance with HIPAA
  - Review of policies generated at University/Hospital Level
    - Clinical, Research and Education Review Groups
  - Educational Activities directed at Faculty & Staff
  - Survey of protected health information at School
  - Infrastructure to ensure data systems security and integrity

http://www.med.stanford.edu/hipaa