HIPAA: In Plain English

Material derived from a presentation by Kris K. Hughes, Esq. Posted with permission from the author.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, was enacted in an effort to redress rising levels of healthcare fraud, ensure portability of health insurance, and facilitate administrative simplification and privacy of patient information within the healthcare delivery industry.

The final regulations promulgated under HIPAA's authority include Standards for Electronic Transactions and Code Sets; Standards for Privacy of Individually Identifiable Health Information. Proposed standards include the forthcoming Security Regulation and Employer and Provider Identifier Standards.

More About the Rules:

Electronic Transaction Standards (Final)
By October 16, 2002, Electronic Transactions must use standardized code sets for encoding data elements when used in connection with "covered transactions." Electronic Transactions are defined as: "The exchange of information between two parties to carry out financial or administrative activities related to health care." These transactions include:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Benefit coordination
- Enrollment in and withdrawal from a health plan
- Eligibility for a health plan
- Health plan premium payments
- First report of injury
- Health claim attachments

Privacy Standards (Final)
The Privacy Rule, effective April 14, 2001, requires compliance by April 14, 2003 for most covered entities. Small health plans have an additional 12 months in which to comply.

Requirements under the Privacy Regulation include:

- Business Associate Agreements
- Consent
- Authorization
- Notice
- Disclosure Audits
- Minimum Necessary Requirements
- Privacy Officer Appointment
- Written Privacy Procedures
- Grievance Procedures

Patient rights granted by the Privacy Rule include:

- Access to health information
- Disclosure accounting
- Notification of Privacy Practices
- Notice of intention and manner in which protected information may be used

Security Standards (Proposed)
The security standards are intended to protect the confidentiality, integrity and availability of healthcare information. To that end, the Rule requires covered entities engaging in the electronic transmission of protected information to implement administrative, technical and physical measures.

While the Final Security Standard is not expected to drastically differ from the proposed version, the information herein references the requirements as found in the Proposed Security Rule.

Key Points:

- Documentation is key to successful evaluation and implementation of the security requirements. Memorializing the steps taken throughout the compliance process will provide a point of reference for future implementation efforts, as well as offer explanatory rationale for both action and inaction with respect to modifications, assessments, and implementation strategies.
- Develop "living" policies and procedures. Stacks of static procedure manuals and guidelines will not be enough to reach adequate levels of compliance. Policies must be regularly reviewed, tested, and revised when necessary.
- The Security Standards were intended to be "technologically neutral" ad scalable in order to provide for future technological and medical advancement. The government could not adequately anticipate, nor subsequently modify the standards to address the technologies available to address the security requirements. Further, the Security standards were intended to affect "covered entities" on a broad scale-each with differing financial, technological and personnel resources.

Administrative Procedures
Administrative procedures are required to guard data integrity, confidentiality and availability. These procedures are documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to data protection.

Administrative Procedure Requirements:

- Certification (internal or external)
- Chain of Trust Partner Agreements
- Contingency Plan: A routinely updated plan for responding to a system emergency that includes:
    - Applications and data criticality analysis (assessment of sensitivity, vulnerabilities, and security of programs and information received, manipulated, stored, and/or transmitted).
    - Data backup plan (documented and routinely updated plan to create and maintain, for a specific period of time, retrievable, exact copies of information).
    - Disaster recovery plan (part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure).
    - Emergency mode operation plan (part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of a fire, vandalism, natural disaster, or system failure).
    - Testing and revision procedures (the documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary).
- Records processing mechanism (documented policies and procedures for the routine, and nonroutine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information).
- Information access control (documented policies and procedures that establish the rules for granting different levels of access).
    - Access authorization (information-use policies and procedures that establish rules for granting access-terminal, transaction, program process, or some other use).
    - Access establishment (security policies and rules that determine a entity's initial right of access to a terminal, transaction, program, process or some other use).
    - Access modification (security policies and rules that determine the types of, and reasons for, modification to an entity's established right of access, to a terminal transaction, program, process, or some other use).

- Internal audit (in-house review of records of system activity (login access, file accesses, security incidents).
- Personnel security
    - Supervision of personnel by authorized, knowledgeable person.
    - Maintaining a record or access authorizations.
    - Assuring that operating and maintenance personnel have proper access authorization.
    - Establishing personnel clearance procedures.
    - Establishing and maintaining personnel security policies and procedures
    - Awareness training
- Security configuration management
    - Documentation
    - Hardware and software installation and maintenance review and testing for security features
    - Inventory
    - Security testing
    - Virus checking
- Security incident procedures
    - Reporting procedures
    - Response procedures
- Security management processes
    - Risk analysis (cost/potential loss balance)
    - Risk management
    - Sanction policies/procedures
    - Security policies
- Termination procedures
    - Changing locks
    - Removal from access lists
- Training
    - Periodic security reminders
    - User education
        - Importance of monitoring login success and failure
        - User responsibility for security of healthcare information
        - Password management
    - Awareness training
        - Password maintenance
        - Incident Reporting
        - Viruses

Technical Security Services
In addition to administrative requirements, technical security services must be deployed to guard data integrity, confidentiality and availability. Technical security services include:

- Access Control Procedures for emergency access-documented instructions for obtaining necessary information during an emergency
- Audit Controls
- Authorization Controls-mechanism to record and examine system activity
- Data Authentication Controls-mechanisms employed to record and examine system activity
- Entity Authentication-(for example, Digital Signatures)
    - Automatic logoff
    - Unique user identifier
    - At least one of the following:
        - Biometric ID
        - Password
        - PIN
        - Telephone callback procedure
        - Token

Technical Security Mechanisms
If using communications or network controls, security standards for technical security mechanisms must include:

- Integrity controls
- Message authentication

And **one** of the following:

- Access controls (transmission protection)
- Encryption

If using network controls for protecting sensitive communication transmitted over open networks, technical security mechanisms must include **all** of the following:

- Alarm
- Audit trails
- Entity authentication

- Event reporting (networking message indicating operating irregularities

Physical Safeguards

- Assigned security responsibility
- Media controls
    - Access control
    - Accountability
    - **Data backup** (a retrievable, exact copy of information)
    - **Data storage** (retention of HCI pertaining to an individual in electronic format).
    - Disposal
- Physical Access Controls
    - Disaster recovery
    - Emergency mode operation
    - Equipment control (hard/software in and out of facility)
    - Facility security plan (guarding against unauthorized access)
    - Access authorization verification procedures
    - Maintenance records
    - Need-to-know procedures (information accessibility limited to necessary, task-specific functions).
    - Sign-in visitor procedures
    - Testing and revision
    - Policy/Guidelines on workstation use
    - Secure workstation location
    - Security awareness training

Third Party Relationships

Trading Partner Agreements-Electronic Transaction Standards
A Trading Partner Agreement is an agreement between business partners, relating to the exchange of information through electronic transactions. This agreement **may** be part of an existing comprehensive agreement addressing similar issues concerning information use and privacy or may be a separate agreement, particular to the requirements of the Electronic Transaction Standard.

Business Associate Agreements- Privacy Rule
This is the method by which covered entities ensure that their business associates, to whom they discloseProtected Health Information (PHI), will handle the information appropriately. Business Associate Agreements require third parties to use PHI in a manner consistent with the purposes for which the information was provided.
Business Associate Agreements (BAA's) must contain, among others, the following provisions:

- Covered Entities must retain the ability to terminate the agreement in the event that a material term of the agreement is violated.
- Covered Entities must retain the authority to terminate the agreement in the event that a material breach cannot be cured otherwise.
- If termination of the agreement is infeasible, Covered Entities are required to contact the DHHS.

Chain of Trust Agreements- Security Standard
This is a contract by which parties agree to electronically exchange data and to protect the transmitted data. Both the sender and the receiver must maintain the integrity and confidentiality of the transmitted information. Each "link in the chain" must maintain the same level of security.

HIPAA Enforcement
Enforcement of HIPAA rules is handled by:

- Office for Civil Rights (civil)
- Department of Justice (criminal)
- "Voluntary Compliance"-the Department has indicated its willingness to work with covered entities to attain compliance, voluntarily. The common goal intended to benefit the healthcare delivery industry, rather than unduly burden it.

The Department of Health and Human Services recently released official "Guidelines" for assistance in implementing and understanding the Privacy Regulation

Civil Penalties	**Criminal Penalties**
- Fines of up to $100,000.00 per violation	Wrongful disclosure of IIHI:
- Maximum fine: $25,000.00 per individual, per violation, per year.	$50,000.00/ 1 year
	$100,000.00/ 5 years
	$250,000.00/ 10 years

Existing Contracts	**New Contracts**
Inventory of existing agreements between covered entities and third parties (i.e. vendors).	HIPAA Considerations: Burden Sharing:
May require renegotiation and/or addendums.	Administration Maintenance Training

Liability

Third-party agreements- regulation violations

- Where will the blame fall?
- Who will be responsible for ensuring accountability and redress for breaches?
- Contractual provisions should anticipate potential liability.

Internal safeguards

- Documentation.
- Continuous Review.
- Thorough Training.
- Reporting Procedures.
- Sanction/ Termination Procedures.

State Law Issues

- Preemption- HIPAA Regulations to serve as a FLOOR. State and Federal Law intersection requires careful legal evaluation.
- Causes of Action- Breach of privacy. Violation of statute as evidence of breach of duty.

Standard of Care

- The level at which information is developed, transmitted, accessed, stored and protected will have a profound impact on health care in terms of “standard of care.”

- The purpose of the Act is to heighten the quality of health care delivery through the simplifying and streamlining of the process.