

HIPAA Compliance

What is HIPAA

- **26 cents of each health care dollar is spent on administrative overhead**
- **Health Insurance Portability & Accountability Act - 1996 Public Law 104-191**
 - **To reform the insurance market and simplify health care administrative processes.**
- **Administrative simplification part of HIPAA**
 - **reduce administrative costs and burdens in the health care industry**
 - **use of standardized, electronic transmission of administrative and financial data.**

What is HIPAA

- **HIPAA requires the Department of Health and Human Services (DHHS)**
 - to adopt national uniform standards for the electronic transmission of certain health information.
- **Another goal:**
 - Increase use/efficiency of computer-to-computer methods of exchanging standard health care information.

Five Areas

- **Electronic Data Interchange (EDI)**
 - **standard format between trading partners.**
 - enrollment, eligibility, payment and remittance advice, claims, health plan premium payments, health claim status, and referral certification and authorization.
- **Code Sets – uniformly document**
 - **Reasons: Why patients are seen?**
 - **What is done to them (procedures)**
- **Identifiers**
 - **health care providers, health plans, employers, and individuals**

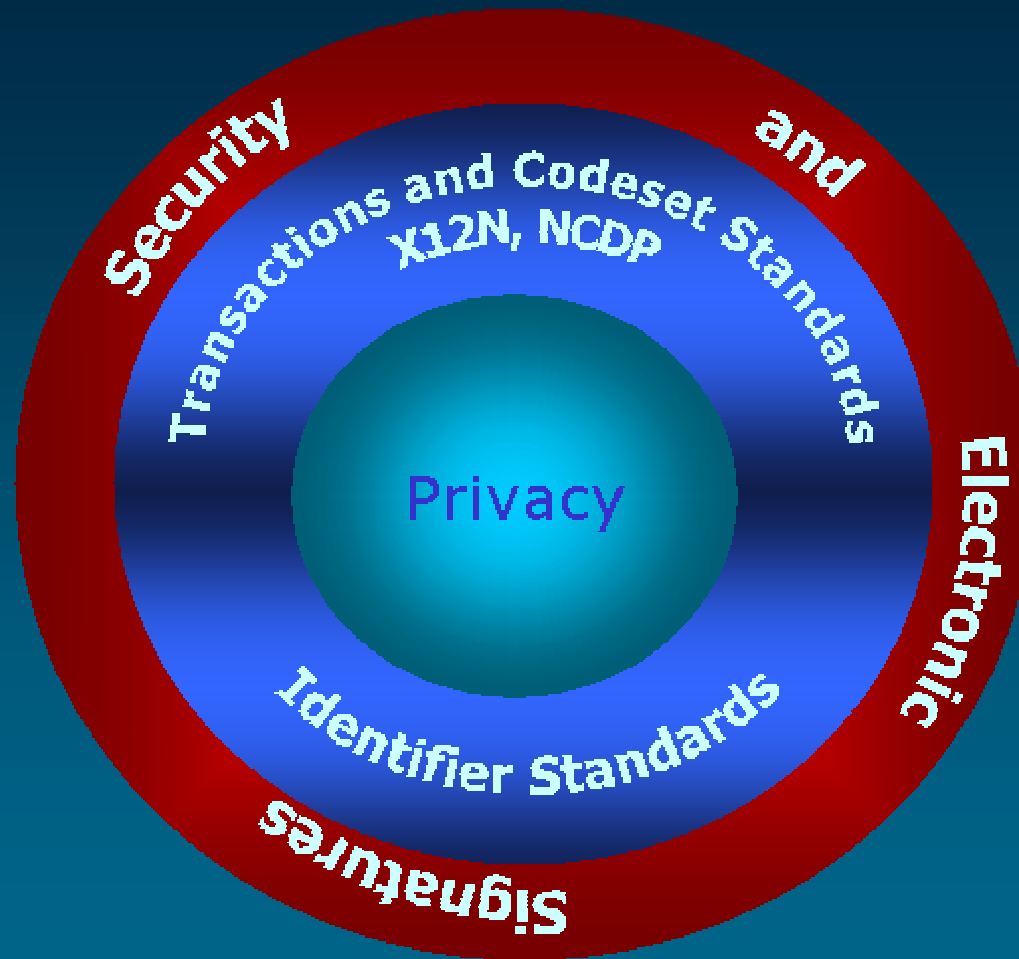
Five Areas

- **Privacy**
 - appropriate and inappropriate disclosures of individually identifiable health information
 - how to protect patient's rights?
- **Security**
 - standards for all health plans, clearinghouses, and providers to follow and to be required at all stages of transmission and storage of health care information to ensure integrity and confidentiality

Who is affected by HIPAA?

- Hospitals
- Insurance Providers
- Healthcare Service Providers
- Clearing Houses
- They are All changing their existing Information systems to comply with EDI, X12N and similar standards defined by HIPAA regulations.

Summary of HIPAA Regulations



Status of HIPAA Standards

HIPAA National Standards	Published	Adopted Standards	Comply By/Small Health Plans
Transactions and Code Set Standards: Final	August 17, 2000	X12N4010, NCDP5.1 (Batch1.0)	October 2002/2003
Privacy Standards: Final	December 28, 2000		April 14, 2003/2004
Security Standards: Proposed	October 13, 1998		
Identifier Standards: NPI, Proposed Rules	NPI: May 7, 1998	8-position alphanumeric identifier Issues by NPS	
Identifier Standards: NEI, Final Rule	NEI: May 31, 2002	EIN (Tax Identification Number)	

Standardization of Code Sets

- **ICD-9-CM**
- **HCPCS**
- **CPT-4**
- **Claim Adjustment Reason Code**
- **Diagnosis Related Group Number (DRG)**
- **Admission Source Code**
- **Admission Type Code**
- **Claim Frequency Type Code**
- **National Drug Code by Format**
- **HCFA Claim Payment Remark Codes**

Transactions Standards

- **Health claims or equivalent encounter information**
- **Health claims attachments**
- **Enrollment and de-enrollment in a health plan**
- **Eligibility for a health plan**
- **Health care payment and remittance advice**
- **Health plan premium payments**
- **First report of injury**
- **Health claim status**
- **Referral certification and authorization**

Privacy

- **HIPAA privacy regulations returns the control of the individual's health information needs to the individual.**
- **We implement the HIPAA privacy solution with the several objectives**

Privacy Objectives

- **Cover all health information, not just that which is or has been transmitted electronically**
- **No health information to be disclosed without the individual's consent or authorization**
- **Provide minimum necessary information required for providing care. This applies except for uses or disclosures made:**
 - **To a health care provider for purposes of treatment**
 - **To the individual**
 - **Pursuant to an authorization**

Healthcare Identifiers

- **Evaluate and Implement the changes due to:**
 - **Final Rules for national employer identifier (NEI).**
 - **Notice of Proposed Rule Making (NPRM) for the national provider identifier (NPI)**
- **Evaluate and implement:**
 - **data quality improvements in registration systems**
 - **data integrity checks on the provider database**
- **Provider Tables:**
 - **Develop procedures to maintain tables**
 - **Integrate or interface tables with necessary systems**

Security: Six categories

- **administrative procedures;**
- **physical safeguards;**
- **security configuration management;**
- **technical security services,**
- **technical mechanisms, and**
- **electronic signatures**

Administrative Procedures:

- **Certification**
- **Chain of trust Partner Agreements**
- **Contingency Plan**
- **Formal Mechanism for Processing Records**
- **Information Access Control**
- **Internal Audit**
- **Personnel Security**

Physical Safeguards

- **Assigned Security Responsibility**
- **Media Controls**
- **Physical Access controls**
- **Policy / Guidelines on Workstation Use**
- **Secure Workstation Location**
- **Security Awareness Training**

Sec. Configuration Management

- Security Incident Procedures
- Security Management Process
- Termination Procedures
- Training

Technical Security Services:

- **Access Controls**
- **Audit Controls**
- **Authorization Controls**
- **Data Authentication**
- **Entity Authentication**

Technical Security Mechanism

- **Communication/Networking Controls**
- **Network Controls**

Electronic Signature

- **Digital Signature**

Requirement	Implementation
Certification	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records	
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt) Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies.