

# HIPAA Awareness Training



# What is HIPAA?

The federal law known as “HIPAA” stands for:

HHealth

Insurance

Portability and

Accountability

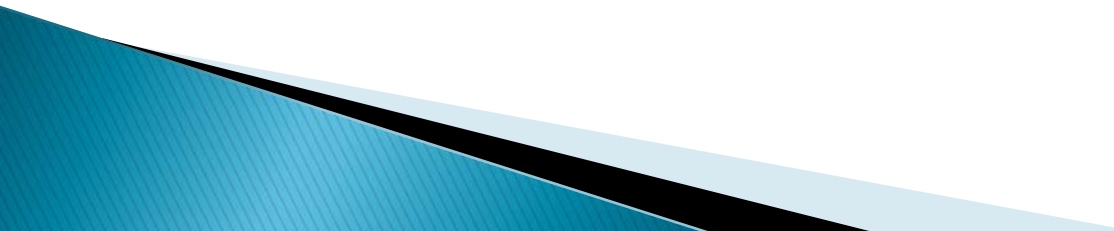
Act of 1996

# What is HIPAA?

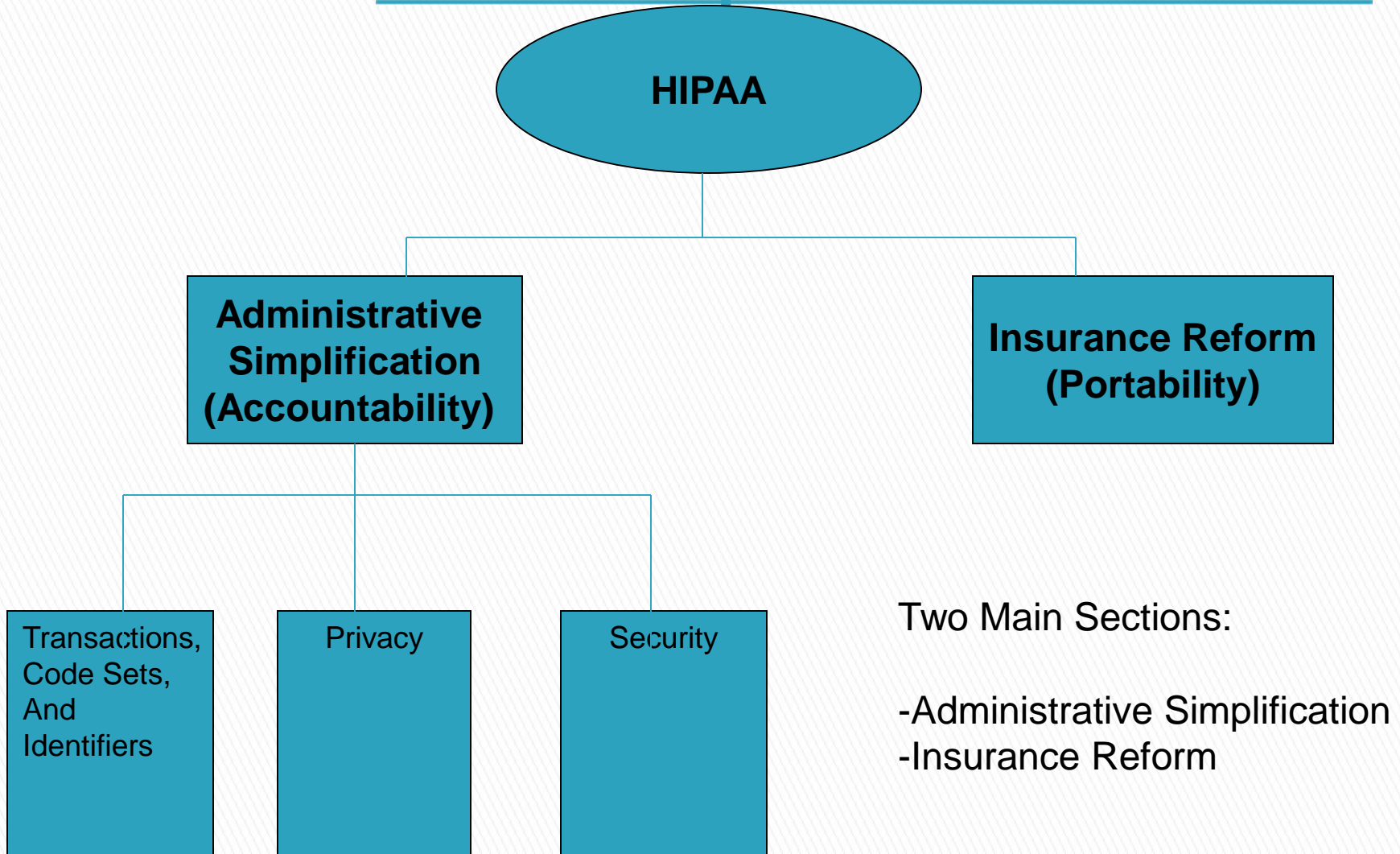
## HIPAA provides:

- Standardized patient health, administrative, & financial information
  - Creation of unique health identifiers in computer systems for e-records
    - Protection & security of confidential patient health information
  - Portability of group sponsored health insurance coverage in certain circumstances
- 
- ▶ It is a law that must be followed by all Healthcare personnel at every level
  - ▶ HIPAA is a set of basic national privacy standards & fair information practices
  - ▶ The purpose of HIPAA is to protect the privacy of all patients in the U.S. who receive any kind of healthcare services
  - ▶ Because of HIPAA, Americans can enjoy a basic level of protection and peace of mind about their healthcare information

# Who Is Affected by HIPAA?

- ✓ Directly Affected: All organizations that directly maintain and transmit protected health information.
  - ✓ Indirectly Affected: All third party vendors and business partners that perform services on behalf of or exchange data with those organizations that directly maintain and/or transmit protected health information.
- 

# The Components of HIPAA



# Administrative Simplification

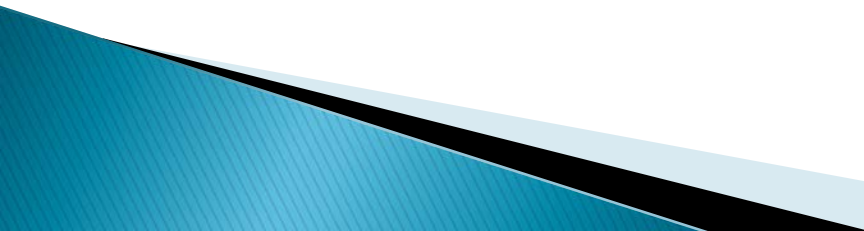
The purpose of Administrative Simplification is:

1. Improve the efficiency and effectiveness of the national health care system
2. Reduce fraud and abuse
3. Protect privacy of health information
4. Protect patient rights
5. Enhance information availability for decision making
6. Reduce the vulnerability of Internet-based technology to security breaches.

Components Include:

- Electronic Transactions, Code Sets, and Unique Identifiers
- Privacy
- Security

# Transactions, Code Sets, and Identifiers

- In an effort to simplify the electronic exchange of financial and administrative health care transactions, the HIPAA transaction standards require all health plans, health care providers, or health care clearinghouses to use or accept the certain electronic transactions
  - HIPAA requires that all health care organizations utilize standardized code sets within these transactions to describe medical data elements
  - For a transaction to be successful, it will require both the sender and the receiver to utilize standard transactions and standard code sets
- 

# HIPAA PRIVACY RULE

- ▶ Privacy refers to what is protected (health information)

AND

- ▶ Who is permitted to use, access, or disclose the information

Protected Health Information (PHI) = personally identifiable health information, linked to a specific person by name or other identifiers in electronic and paper database



# HIPAA PRIVACY RULE

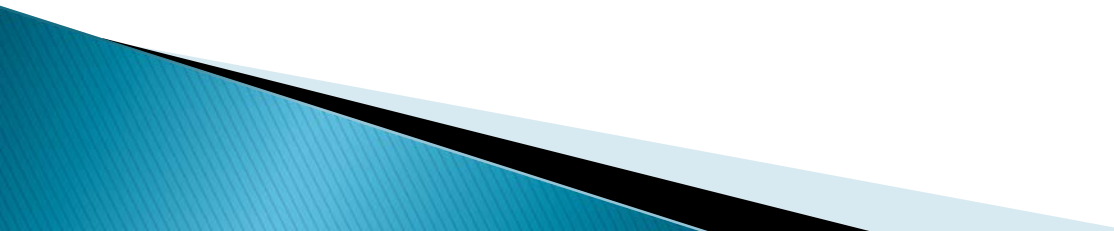
## Administrative Requirements for Privacy:

- ▶ Organizations must have a Privacy Officer
  - ▶ Richard Meyer, MD is the Privacy Officer for PBM Lewisville
- ▶ Organizations must have written contracts with Business Associates which state PHI will be safeguarded
- ▶ Organizations must have policies, procedures and systems in place to protect health information and individual rights
- ▶ Organizations must have on-going training for staff

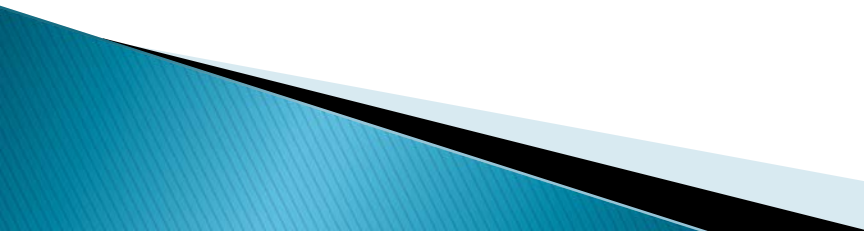
# HIPAA SECURITY RULE

- ▶ The HIPAA Security Rule requires all covered entities to protect the ePHI (*Electronic PHI*) that they use or disclose to other entities
- ▶ This rule imposes numerous responsibilities on covered entities to develop and implement safeguards, policies and procedures to protect electronic PHI
  - ▶ Administrative Safeguards (Risk Analysis, Disaster Recovery Plan)
  - ▶ Physical Safeguards (Facility Access Control)
  - ▶ Technical Safeguards (Unique User Identification, Encryption/Decryption)
  - ▶ Organizational Requirements (Business Associate Agreements)

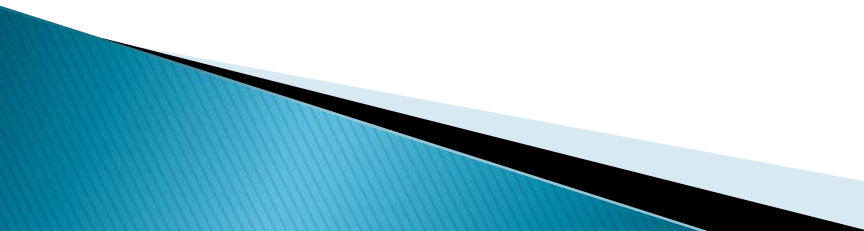
# How does HIPAA affect your job?

- ▶ The way you communicate on the job
  - ▶ The way you use patient healthcare information while performing your job duties
  - ▶ You also must be aware of PBM's specific communication standards, policies and procedures
- 

# Hints to help with HIPAA Compliance

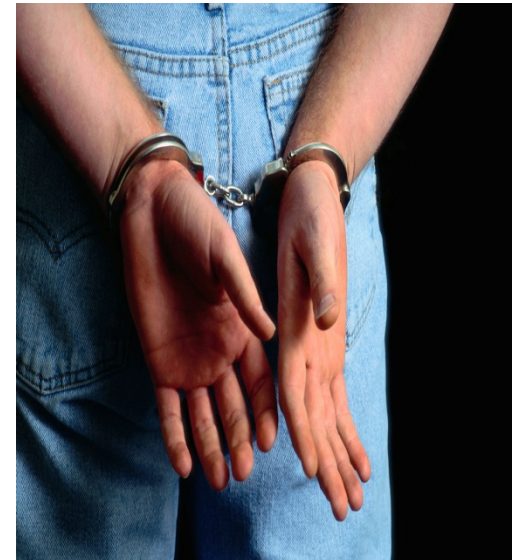
- ▶ Act responsibly with PHI
  - ▶ Do not share information about patients with friends, family, other employees, other patients or other non-authorized individuals
  - ▶ When you need to talk about information for healthcare purposes, check your surroundings and make sure others are not listening
  - ▶ Only access cases which are applicable for your job duties
  - ▶ Ensure paperwork with PHI is not left lying around where vendors or outside visitors can view it
  - ▶ Password protect mobile devices to restrict viewing access
  - ▶ Do not share computer/system log in information or passwords
- 

# The HITECH Act: New Security Breach Notification Requirements

- ▶ The federal stimulus package, signed by Obama 2/17/09, contains the HITECH (Health Information Technology for Economic and Clinical Health Act), which sets forth several changes to the HIPAA
  - ▶ Patients must be notified any time their unsecured PHI may have been compromised through unauthorized acquisition, access, use or disclosure
  - ▶ If a breach affects 500 or more patients, it must be reported to the Department of Health and Human Services, which will post on its website the name of the entity that experienced the breach. Must also be reported to the media
- 

# Results of breaking the regulation

- ▶ Violation of HIPAA carries both civil and criminal penalties. Up to \$1.5 million!
- ▶ If you are aware of a breach in the security or confidentiality of PHI, you should report it to your manager, HR, or assigned Privacy Officer.



# Texas HB 300: A Stricter Standard

- ▶ Texas House Bill 300 – Effective in September 2012
  - ▶ Expansion goes above and beyond federal HIPAA privacy and security rules
  - ▶ Provides administrative, civil, and criminal penalties for the state of Texas
  - ▶ Expands the definition of a covered entity and business associate
  - ▶ Requires employees be trained on how to protect private patient health information within 90 days of employment
  - ▶ When requested by the patient, covered entities must provide the electronic health record within 15 days to the patient
  - ▶ Covered entities will provide notice to patients that protected health information (PHI) is subject to electronic disclosure
  - ▶ PHI is prohibited from disclosures unless for Treatment, Payment, and Operation (T.P.O.) of a healthcare facility
  - ▶ Covered entities must have permission to disclose PHI, except for T.P.O.
  - ▶ PHI held by a governmental agency is NOT public information

# DISCUSSION

»» Questions?