Health Insurance Portability & Accountability Act (HIPAA)

What is HIPAA?

- Kennedy-Kassebaum Bill under President Clinton
- Enacted in 1996 - subsequent laws at different intervals
- Antiquated system of providing health Care

Why HIPAA?

- Increased use of electronic communication and data sharing
- Standardize and simplify electronic sharing of health information
- Increased demand by consumers to protect privacy & security of health information
- Reduce cost, time, and errors in reporting for reimbursement
- Increased regulation over insurance industry

Who does HIPAA apply to?

- Health plans
- Health Clearing houses
- Health care providers/business partners

Major Components

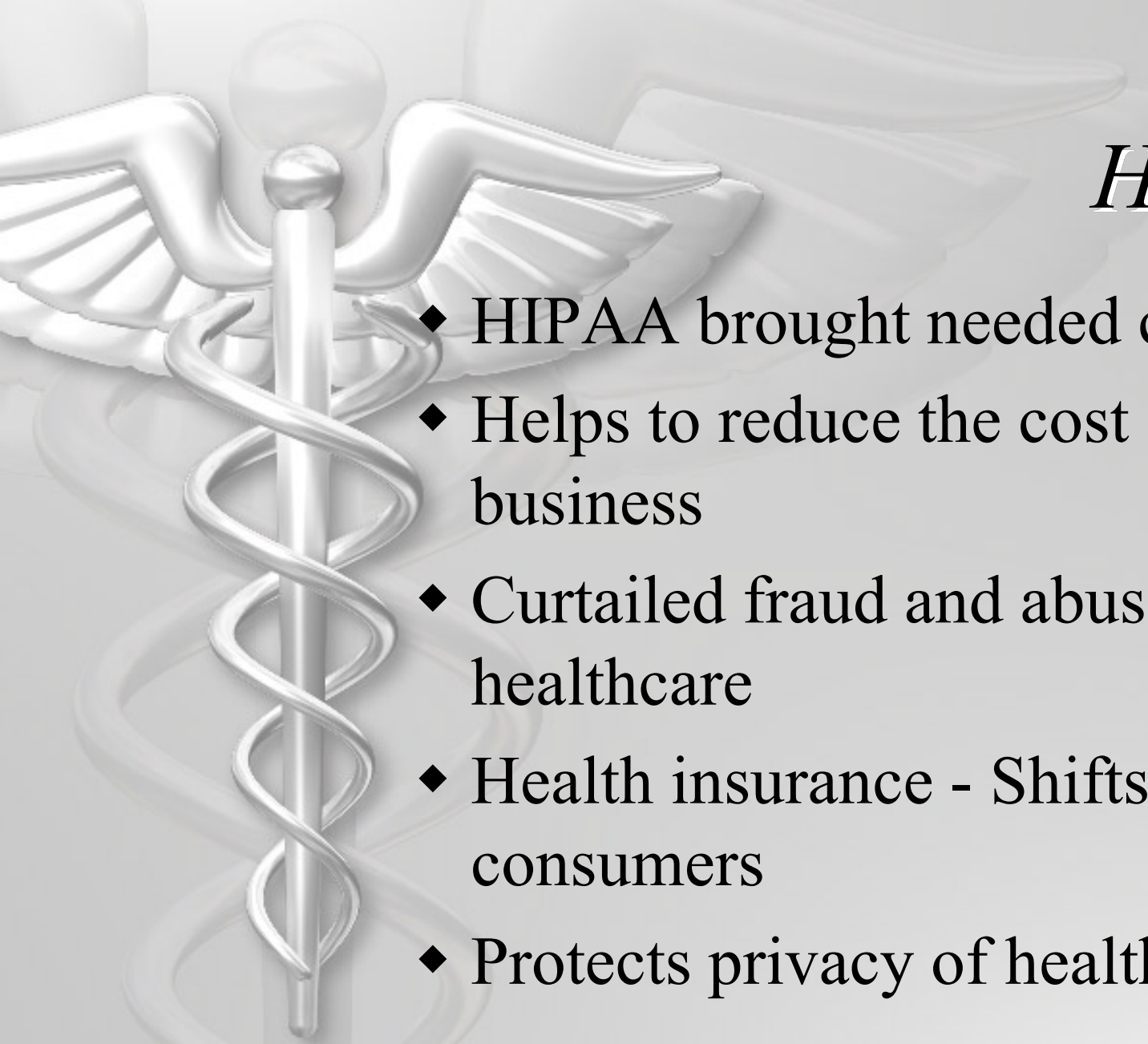
- Title I - Health Care Access, Portability and Renewability
- Title II -
  - Preventing Health Care Fraud and Abuse
  - Medical Liability Reform
  - Administrative Simplification
- Title III - Tax Related Health Provision
- Title IV - Group Health Plan Requirements
- Title V - Revenue Offsets

Assistance with HIPAA

- Website
- Checklist
- Hotlines
- Extensions to deadline

Penalties if not compliant

- HHS excludes provider from Medicare participation
- Civil fines $100 per violation for each provision violated per day; $25,000 CY cap
- Criminal fines $250,000 or 10 yrs. Imprisonment, or both



HIPAA 1

- HIPAA brought needed change
- Helps to reduce the cost of doing business
- Curtailed fraud and abuse in healthcare
- Health insurance - Shifts control to consumers
- Protects privacy of health records

HIPAA II-Health Information Technology for Economic and Clinical Health Act

- HITECH Act-originated from Title XIII of ARRA, 2009.
- HITECH Security Breach notification rule is due to kick off on Feb 22, 2010.
- It applies to all business entities associated with healthcare organizations such as banks, claims, clearing houses, billing firms, health info exchanges, and software companies.

HIPAA II-HITECH RULE

- Breach notification rule
- The major provisions include:
- 60 days notice
- Covered entities, as well as their business associates, must notify individuals within 60 days if protected health information is breached. They also must notify the Department of Health and Human Services and local news media if the breach involves more than 500 individuals.

HIPAA II-HITECH Rule

- Annual report
- Covered entities must maintain a log of all data security breaches and annually submit it to HHS.
- Who reports to whom?
- Business associates experiencing a breach must notify the covered entity, which then must notify the individuals. Companies that sell personal health records, however, must comply with a similar breach notification rule from the Federal Trade Commission.

HIPAA II-HITECH Rule

- Defining "breach"
- According to HITECH, the term "breach" means "the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where the unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."
- Snail mail requirement
- A healthcare organization would

HIPAA II-HITECH Rule

- Snail mail requirement
- A healthcare organization would have to send out a first-class letter to any patients who might have been affected by a breach. (Electronic mail can be used "provided the individual agrees to receive electronic notice and such agreement has not been withdrawn," according to the Interim Final Rule.) If 10 of those first-class letters are returned for a bad address, the hospital must then post notification of the breach on its home page and offer a toll-free breach information number for 90 days, the Interim Final Rule points out. Instead of the Web site posting, an organization could publish a notice of breach in the local news media.

HIPAA II-HITECH Rule

- Important exceptions
- Notification of a breach is not required if the information was unintentionally disclosed to an authorized recipient and not further disclosed.
- Breaches also do not have to be reported if the data involved is rendered unreadable via encryption. Data encryption, however, must be NIST Federal Information Processing 140-2 Standard validated, according to the Interim Final Rule that further spelled out breach notification requirements.
- "Covered entities and business associates should keep encryption keys on a separate device from the data that they encrypt or decrypt," the Interim Final Rule states.

HIPAA II-HITECH Rule

- Harm threshold
- In addition, the Interim Final Rule instituted a "harm threshold" that would dictate when an organization has to notify individuals of a breach. Under this provision, organizations much conduct a risk assessment "to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure." That means federal regulators are largely leaving it up to healthcare organizations to determine if they need to give notification. The provision has been criticized by many privacy advocates and hailed by some healthcare associations

HIPAA II-HITECH Rule

- **Enforcement**
- The Office of Civil Rights within the U.S. Department of Health and Human Services has enforcement authority for the breach notification rule. State attorneys general can bring a civil action in federal court for violations of healthcare security and privacy rules. Victims can receive compensation from fines levied against individuals and organizations.

HIPAA II-HITECH Rule

- **Tougher fines**
- Penalties now can be levied against individuals within a healthcare organization as well as the organization itself. Penalties for breaches of personal healthcare information or other HIPAA violations range up to $1.5 million per violation. This is separate from any criminal penalties that might apply.

HIPAA II-HITECH Rule

- **Accountability**
- Individuals can request that healthcare organizations account for all disclosures of their protected health information from electronic health records systems. This includes information used for treatment, payment and operations. A covered entity may impose a fee for such accounting that's no greater than its cost. The effective date is dependent on when the EHR system was installed.

HIPAA II-HITECH Rule

- **Copies of records**
- Individuals now have the right to receive an electronic copy of their personal health information that's stored in an electronic health record. Healthcare organizations can charge a fee that covers their labor costs for producing the copy.

HIPAA II-HITECH Rule

- **"Minimum necessary" disclosures**
- The HITECH Act specifies that covered entities should limit uses and disclosures of personal health information to the "minimum necessary" to conduct a particular function. The U.S. Department of Health and Human Services is expected to issue regulations this year(2010) governing the "minimum necessary" provisions

HIPAA II-HITECH Rule

- **Marketing restrictions**
- Under the HIPAA privacy rule, when healthcare organizations were paid by companies to send communications to patients about new products and services, they were considered part of the organization's operations, and, thus, were permissible. Under the HITECH Act, these are considered marketing activities and are subject to regulations that will be issued later this year. An exception is permitted if the communication is about a currently prescribed drug and the company's payment to the healthcare organization is "reasonable."