

HIPPA

- “A breach of a person’s health privacy can have significant implications well beyond the physical health of that person, including the loss of a job, alienation of family and friends, the loss of health insurance, and public humiliation.”

Gordon J. Apple

Mary D. Brandt

- The Health Insurance Portability and Accountability Act was made part of Public Law (104-191) on August 21, 1996.
- Its main goal is to encourage health related organizations to establish standards and methods for securely transmitting and handling of sensitive health information

# Privacy Rule

- Requires covered entities to guard against misuse of personally identifiable health information and limit the sharing of such information.
- The Privacy Rule also grants consumers significant rights regarding the use and disclosure of their health information.

# Security Rule

- Requires covered entities to implement basic safeguards to protect electronic protected health information (“PHI”) from unauthorized access, alteration, deletion, and transmission.
- The security standards define the administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI.

# Role Based Access

- While not a requirement under HIPAA, it turns out that some parties may access some data and others may not. Your design should take this into account.

# Protected Health Information (PHI)

- Access to certain fields (PHI) may be restricted, and you'll need to show the steps you took to ensure this information is not released, either accidentally or through foul play. You may also need to track legal access to PHI.

# Archiving

- HIPAA requires archival storage of data, but it doesn't say how long, depending instead on "best practices". Make this selectable, and back up reasoning for this in the documentation.

# Disaster Planning and Recovery

- HIPAA requires that you maintain backups in such a manner that a disaster will neither destroy or limit access to live or archival data for any longer than need be. How long is not stated.

# "Break Glass" Initiative

- HIPAA states that it does not sanction failures in delivery of health care as a result of implementing this law. In this case, it means you can lock down PHI based on roles, or secure in any number of ways, but if a doctor in an ER needs that patient information, there must be a means of overriding security and (a) allowing access to critical PHI as well as (b) tracking that abnormal access. In other words, in an emergency, you need to be able to break the glass and get to the PHI if you need it.

# Risk Assessment

- HIPAA enforcement focuses on intent and due diligence. Even if you make a mistake, it'll go a lot easier on you if you've researched your decisions and documented them in a Risk Assessment.

## TITLE II.F.C--Section 1173

- SAFEGUARDS--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards—
  - (A) to ensure the integrity and confidentiality of the information;
  - (B) to protect against any reasonably anticipated
    - (i) threats or hazards to the security or integrity of the information; and
    - (ii) unauthorized uses or disclosures of the information
  - and
  - (C) otherwise to ensure compliance with this part by the officers and employees of such person.

# SECTION 1177

- **(a) OFFENSE.--**A person who knowingly and in violation of this part—
  - (1) uses or causes to be used a unique health identifier;
  - (2) obtains individually identifiable health information relating to an individual; or
  - (3) discloses individually identifiable health information to another person shall be punished as provided in subsection (b).
- **(b) PENALTIES.--**A person described in subsection (a) shall—
  - (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both;
  - (2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and
  - (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

# HIPAA Scenario

- Mr. Smith goes to the hospital...