HIPAA OVERVIEW

❖ **What is HIPAA?**

- HIPAA = Health Insurance Portability and Accountability Act
- Federal legislation passed in 1996 and amended in 2003 and 2009 to include the HITECH Act, which establishes 4 categories of violations by level of culpability, 4 tiers of penalties, and a maximum penalty of $1.5 million for all violations of an identical provision.
- The University of Arkansas is a covered entity.

❖ **What do we protect?**

Protected health information (PHI) and electronic protected health information (ePHI)

- Health information that contains data elements that identify an individual
- Information that relates to an individual's
  - ✓ Physical or mental health or condition
  - ✓ Healthcare services
  - ✓ Payment for healthcare services
- ***All*** PHI whether it is written, spoken or electronic

❖ **What happens if CES doesn't comply?**

- Electronic violations
  - ✓ Up to $50,000 for each violation and $1.5 million for identical provisions during a calendar year
  - ✓ Up to 10 years imprisonment
- Privacy violations -
  - ✓ Fines up to $250,000
  - ✓ Up to 10 years imprisonment for worst violations

❖ **What happens if you and I don't comply?**

- HIPAA requires the covered entity (U of A) to impose sanctions on employees who don't comply with privacy and security requirements.
- Severity of sanction depends on many factors
  - ✓ Exposure of PHI that results from violation
  - ✓ Intent of employee
  - ✓ Pattern of behavior or one-time mistake?
- Violations can result in termination.

For more information visit
http://www.hhs.gov/ocr/privacy/