Arizona Department of Health Services

The HIPAA Experience

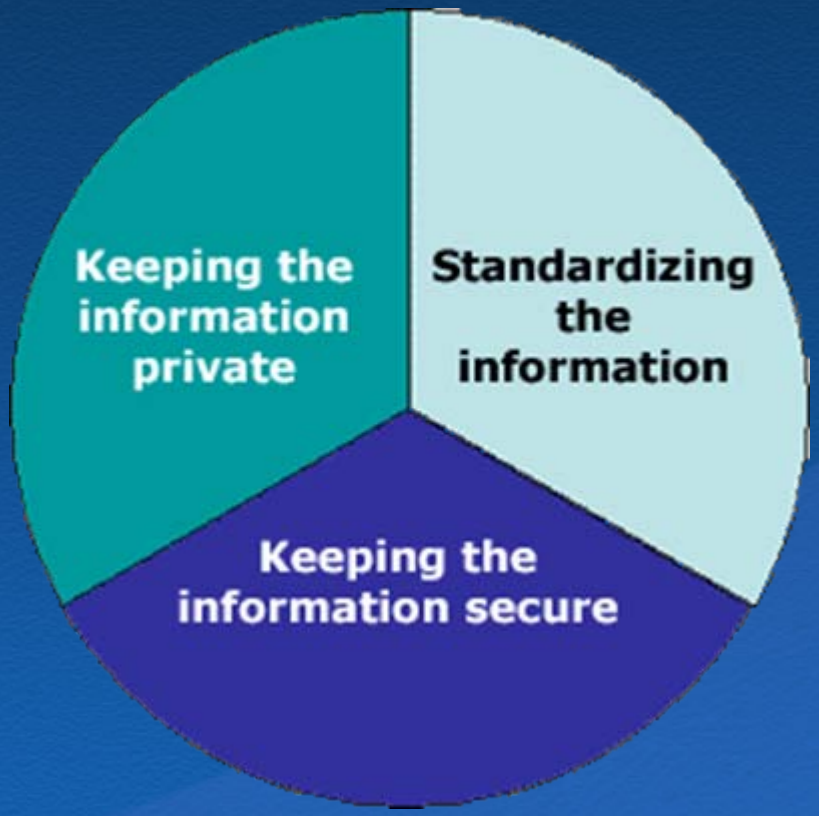
HIPAA Privacy

HIPAA (Health Insurance Portability and Accountability Act) of 1996

Arizona Department of Health Services

The HIPAA Experience

HIPAA Privacy



Arizona Department of Health Services

HIPAA Privacy

Who Must Comply?

- **Covered Entities:** Health care providers, health plans, health care clearinghouses
- **Impact of Compliance:** ADHS receives information from covered entities and is a "hybrid entity"
- **Heavy Penalties for Non-Compliance!**

Arizona Department of Health Services

What is Protected Health Information?

HIPAA Privacy

HIPAA defines <u>Protected Health Information (PHI)</u> as:

- *Individually identifiable health information*
- *Created or received by a health care provider, health plan or health care clearinghouse*
- *Oral or recorded in any form or medium*
- *Relates to past, present or future physical or mental health or condition; the provision of such care; or the payment of such care*
- *Transmitted by electronic media*

Arizona Department of Health Services

HIPAA Privacy

The HIPAA Experience

Privacy Assessment - 2002

Privacy Implementation – April 2003

Plus multiple amendments!

Transaction and Code Sets-

October 2004

Security Assessment/Implementation -

April 2005 (Ongoing)

Arizona Department of Health Services

HIPAA Privacy

HIPAA Security

HIPAA requires that PHI must be **safeguarded** (Secure) when it is requested, used or disclosed.

The HIPAA Security Regulations apply to the physical, technical and administrative safeguards that are implemented to protect the confidentiality, integrity, and availability of the individual's Electronic Protected Health Information **(ePHI).**

Standards: Addressable and Required

Minimum Necessary Requirements

Arizona Department of Health Services

HIPAA Privacy

HIPAA Security

- Gap Analysis:
  - Procedures Policies and Procedures
  - Practices
  - What we thought we were doing!
- Crosswalk of Best Practices
- Addressable versus Required:
  - Response to standards
  - What was needed for ADHS

Arizona Department of Health Services

HIPAA Privacy

HIPAA Security

- Internal/External Environment Assessment (Quasi Penetration Test)
  - Identify locations
  - Identify depth of assessment (how far to penetrate; what are the risks)
  - Prepare the security team but not the workforce….
  - Have a contingency response team

Arizona Department of Health Services

HIPAA Privacy

HIPAA Security

- Perimeter (Internet) Scan
  - Public
  - MAGNET
  - Modems
- Internal Scan
  - Network Systems
  - Phones: War Dialing and Modems
  - Wireless
- Business Partners and “Neighbors”
  - Activities
  - Contracts

Arizona Department of Health Services

HIPAA Privacy

HIPAA Security

- Assessment Process
  - Discovery
  - Light Scanning
  - Heavy Scanning
  - Penetration and Confirmation
- Time Line – 5 to 6 weeks

Arizona Department of Health Services

HIPAA Privacy

Security Remediation

- Documentation and Education
  - Standards
  - Practices
  - Contracts
- Patch Management
- System Hardening
- System Vulnerabilities
- Modem Security
- Wireless Security

Arizona Department of Health Services

HIPAA Experience

HIPAA Privacy

- The Future:
  - Electronic Health Records
  - Health Information Exchange
  - National Provider Identification
  - Regional Health Information Orgs.
  - Arizona Health-e Connection