

# EHR Implementation and Readiness

Are we ready?

# 2004 AHIMA Survey

- Conducted by Healthcare Informatics
- 284 respondents in survey
- 40%- extensively or partially implementing
- 70%- medium or high levels of readiness

# 2004 AHIMA Survey

- Skills required for readiness
  - Process re-engineering
  - Database technologies
  - Project management skills

# 2004 AHIMA Survey

- Applications ranked in order for effective EHR
  - 1. Clinical support systems
  - 2. Clinical documentation
  - 3. Clinical data repository
  - 4. Electronic health record
  - 5. Clinical decision support, CPOE
  - 6. Physician portal
  - 7. RIS, PACS

# 2004 AHIMA Survey

- Major impediments
  - 45% Lack of funding
  - 38% Physician acceptance
  - 13% Lack of standards
  - 4% Low ROI

# HIPAA Security and Regulations

- April 21<sup>st</sup> deadline for HIPAA security compliance
- Security rule based on 3 principles
  - Comprehensiveness
  - Scalability
  - Technology neutrality
- ePHI (electronic personal health information) transmitted in electronic forms
  - Magnetic tapes or disks
  - Optical disks
  - Hard drives
  - Servers

# HIPAA Security and Regulations

- Transmission of ePHI
  - Internet and extranet technology
  - Leased lines
  - Private networks
  - Removable media such as disks
- All security standards must be implemented

# HIPAA Security and Regulations

- Regulations grouped into 5 categories
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational safeguards
  - Policies, procedures and documentation requirements

# Administrative Safeguards

- Security management functions
  - Analyze risks
  - Implement P & P to prevent, detect and correct security violations
  - Define sanctions for security violations
- Assigned Security responsibility
  - Define individual responsible for P & P
- Workforce security
  - P & P for workforce to access appropriate information to perform their job
  - Termination procedures

# Administrative Safeguards

- Information Access Management
  - Implement procedures authorizing access to ePHI
- Security awareness and training
  - Includes workforce and management
- Security incident procedures
  - P & P for reporting and responding to incidents
- Contingency plans
  - Plans for natural disaster
- Evaluation
  - Regular monitoring of adherence to P & P
  - Documentation of results
  - F/U with improvement in P & P

# Administrative Safeguards

- Business associate contracts and other arrangements
  - Contracts must include safeguards to protect ePHI

# Physical Safeguards

- Facility access controls
  - Limitations to access to ePHI including equipment and locations
- Workstation use
  - Include tasks to be performed at each workstation
- Workstation security
  - How workstations permitting access to ePHI are protected from unauthorized use, including portable workstations and PDA's.

# Physical Safeguards

- Device and media controls
  - Must address receipt and removal of hardware and electronic media that contains ePHI

# Technical Safeguards

- Access control
  - P & P limiting access to ePHI to persons or software programs requiring the ePHI to do their jobs
- Audit controls
  - Require installation of hardware, software or manual mechanism to examine activity in systems containing ePHI
- Integrity
  - P & P to protect ePHI from being altered or destroyed

# Technical Safeguards

- Person or Entity authentication
  - Implement measures to prevent unauthorized users from accessing ePHI
- Transmission security
  - Mechanisms to protect ePHI being transmitted electronically from one organization to another

# Organizational Requirements

- Business Associate contracts or other arrangements
  - Must document that they comply with security measures when handling ePHI
- Requirements for group health plans
  - Plan must document safeguards to protect ePHI

# Policies and Procedures and Documentation Requirements

- P & P
  - Reasonable and appropriate
- Documentation
  - P & P must be maintained for period of 6 years from date of creation or when last in effect

# Universal Identifier

- Unique Patient Identifier (UPI)
- Some maintain it's needed for implementing a national electronic MR system
- May improve security and reduce medical errors
- Could separate the identifier process from the access control process
- Layered on top of MR # and EMPI #- it can provide added security

# Universal Identifier

- Naysayers identify problems with data quality, security, cost and politics
- Data quality could be an issue- would we have same problems we now have?
  - Pt. gives incorrect information
  - ID information not with patient
  - DE errors

# Universal Identifier

- Security issues- same dangers as lost SS# or identify theft
- Cost- is infrastructure ready?
- Politics- mandatory or voluntary??

# Where Do You Start?

- Appoint Security Officer
- Conduct Risk Analysis
- Develop Training plan on security awareness
- Check for P & P updates regarding password management and access to information systems
- Ensure you have disaster contingency plans
- Evaluate reuse or destruction of medical information processes such as disk or CD Roms

# Jane's Advice

- Evaluate current HIM practices and storage requirements
- Review all points of origination of documentation
  - Don't forget the Patient Access Department
- Determine amount of current electronic data
  - Lab, Radiology, Pharmacy, Nursing
- Determine role of document imaging and possible cost savings to implement
- Form a Task Force for EHR implementation and include appropriate clinical representation and medical staff representation
- A hybrid environment will most likely be the interim solution
- Don't forget the EHR is a legal document

# HIM Functions- Do they really change??

- Admission and discharge processing and reconciliation
- Deficiency analysis- could be minimized
- Assembly of paper record- re-deployed function for scanning, document preparation, etc.
- Birth and death certificate process
- Coding functions- may be more automated
- Document identification- auditing needed for correct posting of electronic documents
- MPI maintenance- could we use photo ID's of patients?
- Release of information- monitoring required and transition from paper required