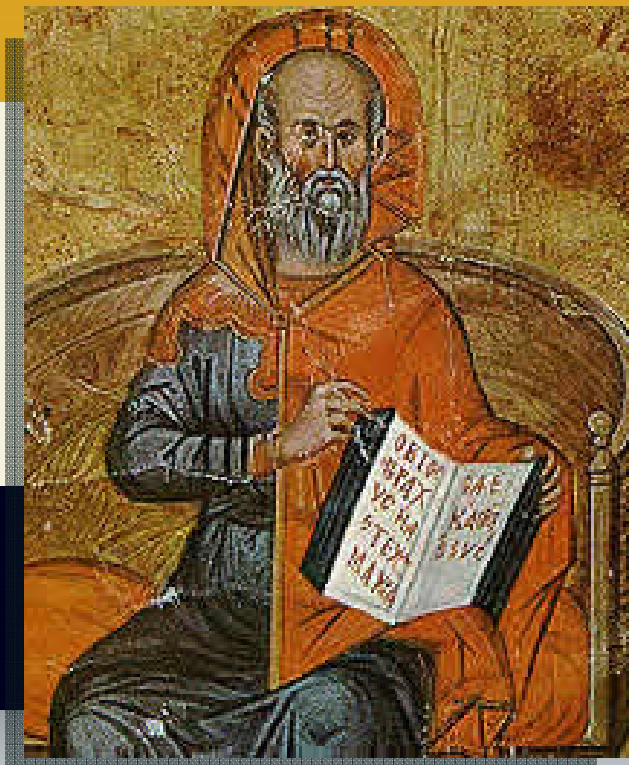
# Health Information Technology and Privilege Management

## *A Policy Agenda for Progress*



**Deborah L. Lafky, Ph.D, CISSP**

**Office of the National Coordinator for Health IT, Office of the Secretary, HHS**

**All material on these slides represents Dr. Lafky's personal viewpoint and not the official position of ONC or HHS.**

# Health Records Systems and HIPAA

- HIPAA is the floor that determines how privileges must be managed in healthcare
  - All “covered entities” are responsible for protecting individually identifiable health information (PHI)
    - the individual’s past, present or future physical or mental health or condition,
    - the provision of health care to the individual, or
    - the past, present, or future payment for the provision of health care to the individual

# Health Records Systems and HIPAA

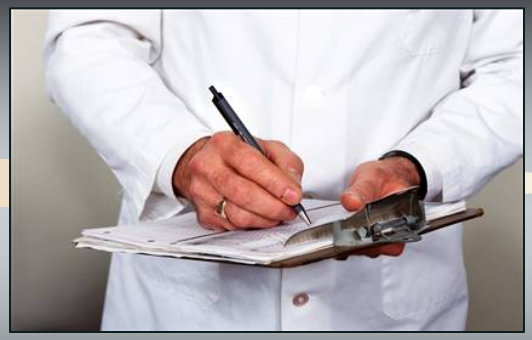
- Permitted uses and disclosures: Treatment, payment, OPERATIONS
  - quality assessment and improvement activities, including case management and care coordination
  - competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation
  - conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs
  - specified insurance functions, such as underwriting, risk rating, and reinsuring risk
  - business planning, development, management, and administration
  - business management and general administrative activities of the entity

# HIPAA and HIT: 1996-2003

- HIPAA passed in 1996
  - In 1996, “Health Information Technology” relied heavily on technology developed between 2000 and 100 BC.

Ink: 2000 BC

Paper: 100 BC



Clipboard: 1963

# 2004-2009

- EO 13335 — 2004
  - Mandated that all Americans will have electronic health records by **2014**
  - Established ONC
    - HITSP
    - NHIN
    - FHA
- ARRA/HITECH — 2009
  - Funding to make these things happen

# The Challenge of HIT

- The goal: health information mobility
  - Reduce redundancy
  - Reduce errors
  - Put information where needed when needed
- The challenge: protecting mobilized health information

# HIT Application Space

- Clinical records (EHR)
- Auxiliary functions
  - E-prescribing
  - Lab
  - Wellness
- Claims management
- Data exchange (HIE)
- Personal health records (PHR)

# Actors in the Space

- Providers
  - Physicians & Surgeons
  - Nurses, nurse practitioners and physician assistants
  - Dentists
- Other licensed professionals
  - Pharmacists
  - EMTs

# Actors in the Space

- Payers
  - Federal government (Medicare, VA, MHS)
  - States (Medicaid)
  - Insurers
- Consumers
- Commercial interests
  - Pharmaceuticals
  - Devices

Medicare becomes law, July 30, 1965

# The Need

To promote a safe and secure health IT infrastructure that assures patient privacy and data integrity while supporting improved health care efficiency and reduced cost.

# The Exposures

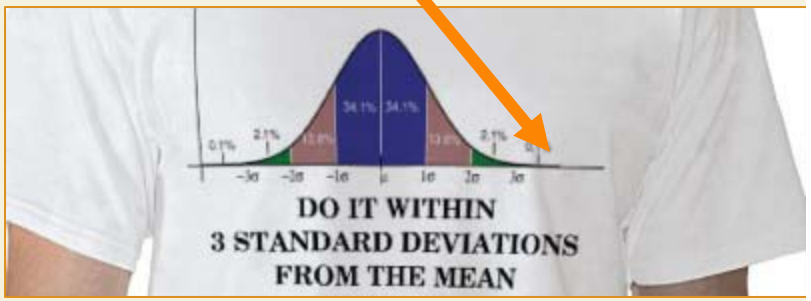
- Data leakage
  - Increased data sharing
  - Heterogeneity
  - Wireless/mobile devices
- Data theft
  - Snooping
  - ID theft
  - Hijacking/extortion

# Potential Consequences

- Health
  - **Compromised data integrity can have life-threatening complications**
- Financial
- Reputation
- Employment
- Criminal activity
  - Drug diversion
  - Fraud

# The Constraints

- State of the industry
  - Healthcare is a very late adopter
  - Fragmented
  - Provider socialization
- Legal
  - Federal and state
- Privacy concerns
  - No uniform patient ID
  - Varying patient preferences
  - The “privacy paradox”



# The Toolbox

- Policy
  - Regulation
  - Legislation
  - Funding
  - Purchasing
- Standards
  - Controlled vocabularies
  - Trust frameworks
  - Messaging

# Deliverables

- Confidentiality
  - Implement consumer preferences at multiple levels of granularity
  - Reconcile consumer preferences with data stewardship requirements
  - Store/transmit preferences without disclosing protected information
  - Respond to queries without disclosing protected information

# Deliverables, cont.

- Assurance
  - Interoperable trust among health care organizations
  - Protected data integrity
- Accountability
  - Iron-clad audit trails
  - Support for multiple levels of entity identity
  - Clear liability rules

# Deliverables, cont.

- Ease of use/transparency
- Low credentialing burden (no Big Brother)
- Low/no cost
- Workflow-friendly

# Questions?