



# HIPAA, Security, and Privacy in Academic Medical Centers: Guidelines for Academic Medical Centers on Security and Privacy (GASP)

---

Presentation for WEDI :

Dave Kirby – Duke University Health System

3/19/2001



## The structure of this presentation

---

- Background
- Guideline section examples up close
- Key Issues for AMCs in HIPAA
- Q&A



# Background

---

- **The idea:** bring representatives from several academic medical centers together in a series of workshops to create guidelines for implementing HIPAA Privacy and Security regulations in AMCs.
- **Also,** use the workshops to explore what AMC needs were in this area and how relevant organizations (e.g. Internet2, AAMC, WEDI, NLM) might find common cause with the AMCs on this issue.
- **The result:** A series of workshops with many nationally known AMCs and related organizations represented in which the guidelines have been developed.
- **Status:** The guidelines have been substantially developed and are nearing publishable quality. Expect a final version in late April 2001 at [amc-hipaa.org](http://amc-hipaa.org) .



# Our purpose today

---

- To describe to you
  - The key results of the workshops to date
  - How these guidelines are expected to be useful to people working on HIPAA in AMCs
  - How the guidelines may be useful to people working on HIPAA in other types of entities.



# HIPAA Covered Entities participating in the workshops

---

- Duke University Health System
- Emory University
- Johns Hopkins Medical Institutions
- Kaiser Permanente
- Mayo Clinic
- Oregon Health Sciences University
- Osaka Medical College
- Texas A&M University System Health Science Center
- Texas A&M University
- University of Alabama at Birmingham
- University of Arizona Medical Center
- University of Michigan Health System
- University of Pennsylvania
- University of Tennessee Health Science Center
- University of Texas Southwestern Medical Center
- Veterans Health Administration
- Yale University School of Medicine



# Sponsoring Organizations

---

- Association of American Medical Colleges (AAMC)
- Internet2
- National Library of Medicine (NLM)
- Object Management Group (OMG)



# Supporting Organizations

---

- CPRI-HOST
- North Carolina Healthcare Information and Communications (NCHICA)
- Health Care Financing Administration (HCFA)
- Healthcare Computing Strategies, Inc. (HCS)
- Southeastern University Research Association (SURA)
- Workgroup on Electronic Data Interchange (WEDI)



# The Goals of the Process

---

- **Develop:** To develop guidelines for implementation of HIPAA Security and Privacy regulations which AMC HIPAA leaders could use to guide their institutional approach.
- **Share:** To share the load and improve the result in an area that we'd otherwise have to take up independently.
- **Focus:** To ensure focus on the special issues that AMCs have with security and privacy.
- **Self-regulate:** To have the guidelines submitted to WEDI for recommendation as part of their regulatory role in HIPAA
- **Norm:** To foster a reasonable group norm on HIPAA compliance for AMCs
- **Collaborate:** To further develop the of points of collaboration with related national groups



# Guideline Structure Overview

---

- Top level categorization for AMC HIPAA Guidelines
- AMC HIPAA Security Guidelines
  - Security Administration
  - Physical Safeguards
  - Technical Security, Services, and Mechanisms
- AMC HIPAA Privacy Guidelines
  - Covered Entities
  - Consent and Authorization
  - Uses and disclosures
  - Consumer Controls
  - Administrative requirements



# Guideline Structure Overview

- **AMC Policy and Management Guidelines**
- A section with discussion and guidance on the larger issues related to HIPAA compliance

Roles and Responsibilities in Development and Maintenance	HIPAA Accreditation Intersections
Developing Support for the HIPAA program	Stricter State Law
Resources for Development and Maintenance	Policy Establishment
Evaluation and Monitoring of Development and Maintenance	Policy Modification
Reasonableness	Policy Usage Introduction
Digital Signature	Privacy Culture



# Format of a guideline section:

---

- Name § Citation
- HIPAA Requirement from regulation
- AMC Explanation of HIPAA Requirement
- Key Issues
- Category I and Category II Guidelines
- Roadblocks
- Comments



# Two Guideline Points- Close up

---



This point addresses the process for internal audit of system activity records.

# SEC.06 Internal Audit:308(a)(6)

## HIPAA Requirement

*Each entity designated in § 142.302 must assess potential risks and vulnerabilities to the individual health data in its possession and develop, implement, and maintain appropriate security measures. These measures must be documented and kept current, and must include, at a minimum, the following requirements and implementation features:*

### **(6) Internal audit**

*(in-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization).*

## AMC Explanation of HIPAA Requirement

Each organization is required to maintain an on-going internal audit process to review records of system activity (for example, logins, file accesses, security incidents) maintained by the organization.



## SEC.06 Internal Audit .308(a)(6) *continued*

---

### Key Issues

- At what level in data structures should audits be maintained. Table? Record? Field?
- How will this degrade performance?
- What data will have logs maintained?
- How often will audits occur?



## SEC.06 Internal Audit .308(a)(6) *continued*

---

### Category I Guidelines-Actions must be taken to address these

- Organizations must periodically review audit trails or activity logs for critical application systems, including user written applications
- Organizations must follow up on suspicious entries such as unauthorized accesses and attempts
- Organizations must identify and resolve inappropriate activity



## SEC.06 Internal Audit .308(a)(6) *continued*

---

Category 2 Guidelines-Actions should be taken to address these

- Audit procedures should validate input data, internal processing and output data
- Audit requirements and activities should not disrupt important business processes
- Appropriate management should agree to and endorse audit tools
- The scope of the checks should be agreed and controlled



## SEC.06 Internal Audit .308(a)(6) *continued*

---

### Roadblocks

Depending on the type of audit desired, vendors may not have the desired functionality/performance.

### Comments

- Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organizational assets.
- Audit trails may become evidence in legal proceedings. Care should be taken to preserve.
- Overlaps significantly with E.02 "Audit Controls"



# PRIV.52 Safeguards 164.530(c)

---

Implementing safeguards to protect health information from intentional or accidental misuse; (Defining User privilege, Authentication, Data Protection, Authorization)

## HIPAA Requirement

(1) Standards: safeguards.

*A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.*

(2) Implementation specification: safeguards.

*A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.*



## PRIV.52 Safeguards 164.530(c) *continued*

---

### AMC Explanation of HIPAA Requirement

A covered entity must establish administrative, technical, and physical safeguards to protect the privacy of protected health information from unauthorized access or use. *The extent of these safeguards is that they must be appropriate and reasonable.*

A group health plan is excepted from coverage by 164.530© in circumstances where it gets limited amounts of protected health information under conditions described in 164.530(k).



## PRIV.52 Safeguards 164.530(c) *continued*

---

### Key Issues

- How should a covered entity handle the determination of what is reasonable and appropriate?
- Is implementing the (proposed) Security regulations an adequate way to address this point in the privacy regulations?



PRIV.52 Safeguards 164.530(c) *continued*

---

Category I Guidelines-Actions must be taken to address these

- A covered entity must establish administrative, technical, and physical safeguards to protect the privacy of protected health information from unauthorized access or use. The extent of these safeguards is that it must be appropriate and reasonable.



## PRIV.52 Safeguards 164.530(c) *continued*

---

### Category 2 Guidelines-Actions should be taken to address these

- AMCs should perform a risk analysis and create and implement a risk management plan for their electronic and non-electronic information assets.
- Privacy official shall consult on safeguard requirements with security official (and others responsible for information practices)
- Privacy official shall enumerate list of reasonably anticipated threats and hazards to privacy of info and unauthorized uses and disclosures

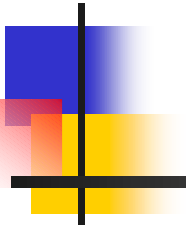
## Roadblocks

The complexity of implementing detailed access control may be difficult for AMCs to implement across their organizations. This is particularly true for legacy systems with inadequate rights differentiation for users.

## Comments

This requirement is an overarching requirement making the covered entity responsible for reasonable privacy safeguards. The Security regs and other aspects of the Privacy regs provide some of the specifics of what safeguarding entails.

# Key Issues for AMCs in HIPAA



# HIPAA:

## Key Issues for AMCs

---

- Organizational Issues:
  - Multi-entity, Decentralized management, Governing Board understanding
- University Affiliations:
  - Decision by committee, Academic culture, Non-employee users
- Multiple Missions:
  - Strain and confusion

# HIPAA:

## Key Issues for AMCs

---

- Organizational:
  - Entity definition, Developing & Maintenance of Roles, Resources, and Eval and Monitoring Process
- Reasonableness and Scalability
- Uses and Disclosures of De-identified Health Information
- Uses and Disclosures for Research Purposes



# HIPAA: Organizational Issues

---

- Entity Definition:
- Developing & Maintenance - Roles
- Developing & Maintenance - Resources
- Developing & Maintenance - Eval and Monitoring Process

# HIPAA:

## Key Issues for AMCs

---

- Reasonableness and Scalability
  - Who will determine what is reasonable
  - What are mechanisms to determine reasonableness

# HIPAA:

## Key Issues for AMCs

---

- De-identified Health Information
  - Requires Expertise
  - Low Risk
  - Removal of specific data elements

# HIPAA:

## Key Issues for AMCs

---

- Uses and Disclosures for Research Purposes
  - Requires documentation of a waiver by IRB or a Defined Privacy Board
  - Documentation must meet specific requirements: ID and Date, waiver criteria, Description of protected HI needed, Review and approval procedures.

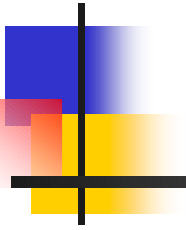
# HIPAA:

## Key Issues for AMCs: Misc.

---

- Compliance Issue: AMCs are accomplished at dealing with compliance
- Incorporation into educational activities in SOM, SON...
- Benchmark between AMCs
- HIPAA as an opportunity

# Q&A



# Do we *HAVE* to do HIPAA?

## Why?

---

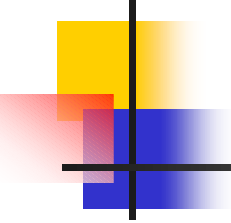
- HIPAA Security and Privacy regulation exist for good reasons.
- These reasons include:
  - Information is a valuable asset of your organization
  - Risk and liability reduction for organization
  - Enhance professionalism and trustworthiness



# What are the HIPAA deadlines that we need to pay attention to for Security and Privacy?

---

- Security regulation is not yet published
- No Security deadline as of today
  - However, anticipated date of spring/summer 2001 for security regulation
  - Compliance date anticipated for mid-2003.
- Privacy regulation published December 28, 2000.
- Privacy compliance date of April 14, 2003



# How will these guidelines be used in developing my organization's approach to HIPAA security and privacy?

---

- Assign roles, responsibilities, accountability
- Risk analysis
- Security program
- Privacy program
- Train staff and organization change



# What is REASONABLE for my organization, in regard to HIPAA Security and Privacy regulation requirement compliance?

---

- Assignment of responsibilities
- Define and introduce policies
- Analyze risks to security and privacy
- Certify security controls
- Scalability (cost burden of implementation)
- Minimum use or disclosure
- Managing consumer requests
- Legal contracts should be updated
- Disclosure and de-identified information



# What are the key HIPAA activities for security and privacy?

---

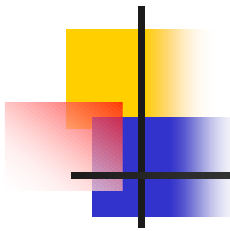
- Review the framework for complying with the regulation.
- Sequence of activities
- Give a few specific examples



# How will you deal with serious organizational issues on the way to compliance?

---

- Organizational structure
- Changing practices
- Financial
- Locating resources
- Interpretation
- Research and Education
- Fundraising and Marketing



# What are the costs versus benefits of HIPAA security and privacy compliance?

---

- Costs:
  - There will be costs associated with any compliance program
  - Increased paperwork for personal health information mechanisms
- Benefits:
  - Reduce business risks
  - Increase consumer trust
  - Reduce exposure to liabilities



# The End

---

- Thanks for your attention.
- Dave Kirby
- 919-272-1157
- Kirby001@mc.duke.edu