

## What should I do first?

### Start planning immediately!

- n Organize for the long term
- n Compliance will be a complex activity coordinate across your enterprise
- n Read "*Guidelines for Academic Medical Centers on Security and Privacy: Practical Strategies for Addressing the Health Insurance Portability and Accountability Act*" for more information and advice

HIPAA Security and Privacy are not one-time implementation projects. They are ongoing responsibilities and they need to be incorporated in to corporate culture and business processes.

## Where can I learn more?

### HIPAA Resources

- n US Dept. of Health and Human Services  
Administrative Simplification  
<http://aspe.os.dhhs.gov/admsimp/>
- n HIPAA Privacy Rule (Final)  
<http://aspe.os.dhhs.gov/admsimp/final/PvcFRpdf.zip>
- n HIPAA Security Rule (Proposed)  
<http://aspe.os.dhhs.gov/admsimp/nprm/seclist.htm>

### HIPAA QUESTIONS & ANSWERS SUMMARIZED FROM

Guidelines for Academic Medical Centers on Security and Privacy: Practical Strategies for Addressing the New Health Insurance Portability & Accountability Act (HIPAA) Regulations.

*To be published Spring 2001*

For additional information see:  
<http://amc-hipaa.org>

Copyright © 2001 AMC-HIPAA  
All Rights Reserved

## Participating Organizations

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  
Tufts University School of Medicine  
University of Alabama at Birmingham  
University of Arizona Medical Center  
University of Michigan Health System  
University of Pennsylvania School of Medicine  
University of Tennessee Health Science Center  
University of Texas Southwestern Medical Center  
Veterans Health Administration  
Yale University School of Medicine

## Supporting Organizations

CPRI-HOST  
Healthcare Computing Strategies, Inc.  
Health Care Financing Administration  
North Carolina Healthcare Information and Communications Association  
Southeastern University Research Association  
Workgroup for Electronic Data Interchange

## Sponsoring Organizations

Association of American Medical Colleges  
Internet2  
National Library of Medicine  
Object Management Group

# GUIDELINES FOR ACADEMIC MEDICAL CENTERS ON SECURITY AND PRIVACY

Practical Strategies for Addressing the Health Insurance Portability & Accountability Act (HIPAA) Regulations



# HIPAA Q&A

## What's the purpose of the HIPAA Security and Privacy Regulations?

To prevent inappropriate use and disclosure of individuals' health information.

To require organizations which use health information to protect that information and the systems which store, transmit, and process it.

## Do the HIPAA Security and Privacy requirements apply to me? When?

Yes, if you are (or have a unit which is):

- n health provider
- n health plan
- n healthcare clearinghouse

Maybe, if you are affiliated with a health provider, health plan, or healthcare clearinghouse as:

- n a business associate
- n a contractor
- n a consultant
- n a researcher using personally identifiable health information

### Compliance Deadlines

If the requirements do apply, you must comply within 26 months after publication of the final rules (April 14, 2003)

- n Small health plans have 36 months to comply (April 14, 2004)

## What are HIPAA Security and Privacy?

### HIPAA Security:

Requires assignment of responsibility for security for health information:

Maintaining reasonable and appropriate safeguards, to:

- n ensure integrity and confidentiality of all health care information which is maintained or transmitted in electronic form;
- n protect against reasonably anticipated threats or hazards to security and integrity of information;
- n protect against reasonably anticipated unauthorized uses or disclosures of information;
- n ensure compliance to safeguards by officers and employees.

Requires assessing risks to confidentiality and integrity of health information.

Requires implementation and documentation of specific:

- n administrative security procedures;
- n physical security safe guards;
- n technical security services;
- n technical security mechanisms.

### HIPAA Privacy:

Requires appointment of a Privacy officer and restricts use and disclosure:

1. by a covered entity
2. of protected health information
  - in any form (including oral communication)
  - psychotherapy notes are given special protection
3. to the minimum information necessary to accomplish the purpose for which the information is used or disclosed but any disclosure to a provider for purposes of treatment is permitted

Defines certain required disclosures.

Defines rights of individuals with respect to information about themselves:

- n right to written notice of information practices;
- n rights of access, review, and correction;
- n right to an accounting of disclosures not for provision of care.

## What should I do about HIPAA Security and Privacy?

Implement a HIPAA security and privacy compliance program.

Security and privacy are policy and compliance issues not just technology issues.

- n Establish a plan and a timeline for compliance
- n Designate a privacy officer
- n Identify a security officer or officers
- n Create a HIPAA security and privacy compliance oversight committee involving all stakeholders (including security and privacy officers)
- n Assign clear responsibility for formulating and implementing security and privacy policy
- n Insure that procedures include risk assessment
- n Train all personnel in security and privacy policies and procedures including contractors and business associates on premises
- n Create (or update) a security and privacy awareness program
- n Review security and privacy policies and procedures periodically
- n Review agreements for HIPAA compliance
- n Review trading partner agreements for conformance to security regulation
- n Review business associate agreements for conformance to privacy regulation
- n Benchmark other similar organizations' security and privacy practices

## What are the penalties if I don't comply with HIPAA Security and Privacy?

- n Civil monetary penalties on a per-person, per violation basis
- n Strong penalties for misuse with knowledge and intent significant fines and prison terms
- n Penalties may apply to the individual violator but they may also apply to the organization or even to its officers