What should I do first?

Start planning immediately!
- Organize for the long term
- Compliance will be a complex activity coordinate across your enterprise
- 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 into corporate culture and business processes.

Where can I learn more?

HIPAA Resources
- US Dept. of Health and Human Services
  Administrative Simplification
  http://aspe.os.dhhs.gov/admsimp/
- HIPAA Privacy Rule (Final)
  http://aspe.os.dhhs.gov/admsimp/final/
- HIPAA Security Rule (Proposed)
  http://aspe.os.dhhs.gov/admsimp/nprm/
  ncpfrpdf.zip
- HIPAA Security Rule (Proposed)
  http://aspe.os.dhhs.gov/admsimp/nprm/
  sec1st.htm

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
- 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
- Internet 2
- National Library of Medicine
- Object Management Group

HIPAA QUESTIONS & ANSWERS
SUMMARIZED FROM
To be published Spring 2001.
For additional information see:
http://amc-hipaa.org

Copyright © 2001 AMC-HIPAA
All Rights Reserved
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):
- health provider
- health plan
- healthcare clearinghouse

Maybe, if you are affiliated with a health provider, health plan, or healthcare clearinghouse as:
- a business associate
- a contractor
- a consultant
- 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.
Small health plans have 36 months to comply.

What are HIPAA Security and Privacy?

HIPAA Security:
Requires assignment of responsibility for security for health information:
- Maintaining reasonable and appropriate safeguards to:
  - ensure integrity and confidentiality of all health care information which is maintained or transmitted in electronic form;
  - protect against reasonably anticipated threats or hazards to security and integrity of information;
  - protect against reasonably anticipated unauthorized uses or disclosures of information;
  - ensure compliance to safeguards by officers and employees.

Requires assessing risks to confidentiality and integrity of health information.
Requires implementation and documentation of specific:
- administrative security procedures;
- physical security safeguards;
- technical security services;
- 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

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

What are the penalties if I don't comply with HIPAA Security and Privacy?
- Civil monetary penalties on a per-person, per-violation basis
- Strong penalties for misuse with knowledge and intent significant fines and prison terms
- Penalties may apply to the individual violator but they may also apply to the organization or even to its officers