Tools to Help Address HIPAA Privacy and Security Regulations

Ted Cooper, MD
National Director
Confidentiality & Security
Kaiser Permanente
HIPAA Security & Privacy Standards Requirements

• We must
  – Perform and thoroughly document formal risk assessment and management efforts to determine the policies, procedures and technology to deploy to address the standards.
  – We must assess the types and amounts of risk that we have, which we will mitigate with policy, procedure and/or technology, and understand what risks remain and that we are willing to accept (i.e. those that will not be addressed completely)
  – Assign responsibility for meeting the standards to specific individuals.
HIPAA Standards for Security & Privacy

While these are called the HIPAA Security and Privacy Standards, the “standard” simply means that we must address their requirements. For the most part both standards are not explicit on the extent to which a particular entity should implement specific policies, procedures or technology. Instead, they require each affected entity to assess its own security and privacy needs and risks and then devise, implement and maintain appropriate measures as business decisions.
Tools

• CPRI Toolkit: Managing Information Security in Health Care
• CPRI-HOST Confidentiality and Security Training Video
• NCHICA’s HIPAA EarlyView™
• NCHICA’s
• ISO/IEC 17799 Code of practice for information security management
• SEI’s CERT Security Improvement Modules & Self Risk Assessment
• GASP Generally Accepted System Security Principles
• SANS Institute Model Policies
• WEDI’s SNIP
• AAMC Guidelines for Academic Medical Centers on Security and Privacy
• PSN HIPAA Privacy and Calculator
The CPRI Toolkit: Managing Information Security in Health Care

• A Resource
• Its Origin
• Third Version of Toolkit
• http://www.cpri-host.org
• How to use it to address HIPAA confidentiality and security
CPRI Toolkit
Content Committee

- Ted Cooper, M.D., Chair - Kaiser Permanente
- Jeff Collmann, Ph. D., Editor - Georgetown U.
- Barbara Demster, MS, RRA - WebMD
- John Fanning - DHHS
- Jack Hueter - CHE
- Shannah Koss - IBM
- Elmars “Marty” Laksbergs, CISSP - Netigy
- John Parmigiani - HCFA
- Harry Rhodes - AHMIA
- Paul Schyve, MD - JCAHO
Goal

• Build security capable organizations!
• Incorporate sound security practices in the everyday work of all members of the organization, including the patient.

• NOT JUST implement security measures!
Security Program Functions

- Monitor changing laws, rules and regulations
- Update data security policies, procedures and practices
- Chose and deploy technology
- Enhance patient understanding and acceptance
How does the *Toolkit* help?

- Regulatory requirements
- CPRI booklets
  - How to go about it
  - What to consider
- Case studies & examples of colleagues’ work
Table of Contents

CPRI Toolkit - Managing Information Security in Health Care, Version 3

- Download Entire Toolkit in Adobe Acrobat - PDF Format (1.58 MB)
- Executive Summary
Toolkit - Sections 1 & 2

Table of Contents

- **PDF** Download Entire Toolkit in Adobe Acrobat - PDF Format (1.58 MB)

- **PDF** 1.0 Executive Summary

- **PDF** 2.0 Introduction
  - 2.1 How to Use This Toolkit
3.0 Monitoring Laws, Regulations, and Standards

3.1 Introduction

3.2 Summary of Proposed DHHS Rules
   3.2.2 Common Elements
   3.2.3 Proposed Data Security and Electronic Signature Standards
   3.2.4 Electronic Transactions/Codes Sets
   3.2.5 Health Care Provider Identifier
   3.2.6 Employer Identifier
   3.2.7 Health Plan Identifier
   3.2.8 Unique Health Identifier - Individuals

3.3 Final Federal HIPAA Security & Electronic Signature Standard

3.4 Federal Medical Privacy Legislation
   3.4.1 Summary of DHHS Confidentiality Recommendations
   3.4.2 Privacy Notice of Proposed Rule Making

3.5 State Medical Privacy Legislation

3.6 Setting Standards in Health Care Information (12/15/1999)

3.7 JCAHO/NCQA Recommendations for Protecting Personal Health Information

3.8 EU Privacy Directive (updated May 2000)
4.0 Developing Policies, Procedures, and Practices

4.1 Introduction

4.2 CPRI Guidelines - Information Security Policies

4.3 Sample Security Policies
   4.3.1 Harvard Vanguard Medical Associates
   4.3.2 Kaiser Permanente Northern California
   4.3.3 Mayo Clinic
   4.3.4 Partners Healthcare System
   4.3.5 PCASSO Security Policy Model
   4.3.6 Project Phoenix, Georgetown University

4.4 Assigning Roles and Responsibilities
   4.4.1 Introduction

4.5 Risk Assessment & Management (updated May 2000)
   4.5.1 Case Study: Project Phoenix - Risk Analysis of a Telemedicine System
   4.5.2 Case Study: Project Phoenix - Risk Management Plan
Toolkit - Section 4.6 - 4.10

4.6 Organizing Security Training
   4.6.1 CPRI Guide - Information Security Education
   4.6.2 Sample Training Materials
      4.6.2.1 Instructor Guide
   4.6.2.2 Slides for Training Program (HTML)
   4.6.2.2 Slides for Training Program (Download Powerpoint)
   4.6.3 Conferences on Information Security Training

4.7 Additional Resources

4.8 Enforcing Security Policies
   4.8.1 CPRI Sample Confidentiality Statements & Agreement
   4.8.2 Case Study: Securing User Agreement at Kaiser Permanente Northern California

4.9 Implementing Information Security Policies
   4.9.1 CPRI Guide — Security Features
   4.9.2 Special Issues in Electronic Transmission of Confidential Data
      4.9.2.1 Fax — Special Issues in Electronic Transmission
   4.9.2.2 Email
   4.9.2.3 HCFA and the Internet
   4.9.3 Case Study: Patient Centered Access To Secure Systems Online (PCASSO)
   4.9.4 CHIME-PKI (updated May 2000)

4.10 Business Continuity & Disaster Recovery (updated May 2000)
5.0 Enhancing Patient Understanding
   5.1 Introduction
   5.2 Complying with Consent, Inspection, and Disclosure Requirements
   5.3 HelpBot: Complying with Patient Education Requirements

6.0 Institutionalizing Responsibility
   6.1 Introduction
   6.2 Case Study: Trustee/Custodian Agreements at Kaiser Permanente

7.0 Web Sites

8.0 Glossary

9.0 Bibliography
Critical Steps in Process

1. Decide what to do
2. Assign security responsibilities
3. Build risk management capability
4. Drive enterprise-wide awareness
5. Enforce policies & procedures
6. Design, revise & validate infrastructure
7. Institutionalize responsibility & support
8. Enhancing patient understanding

HIPAA Deadline: 2003 ??
Toolkit & Critical Steps

1. Deciding what to do

- **Understand the Regulations** - 3
- **Information Security Policies** - 4.2
  - Describes how to develop policies
  - Identifies areas policies should address
  - Security policy examples - 4.3.1 to 4.3.6
Know the Laws, Rules & Regulations

• HIPAA
  – Security Rules - 3.1
  – Medical Privacy - 3.2
• State Medical Privacy Laws - 3.3
• Setting Standards - 3.4
• JCAHO/NCQA Recommendations - 3.5
• EU Privacy Directive - “Safe harbor”
3.0 Monitoring Laws, Regulations, and Standards

3.1 Introduction

3.2 Summary of Proposed DHHS Rules
   3.2.2 Common Elements
   3.2.3 Proposed Data Security and Electronic Signature Standards
   3.2.4 Electronic Transactions/Codes Sets
   3.2.5 Health Care Provider Identifier
   3.2.6 Employer Identifier
   3.2.7 Health Plan Identifier
   3.2.8 Unique Health Identifier - Individuals

3.3 Final Federal HIPAA Security & Electronic Signature Standard

3.4 Federal Medical Privacy Legislation
   3.4.1 Summary of DHHS Confidentiality Recommendations
   3.4.2 Privacy Notice of Proposed Rule Making

3.5 State Medical Privacy Legislation

3.6 Setting Standards in Health Care Information (12/15/1999)

3.7 JCAHO/NCQA Recommendations for Protecting Personal Health Information

3.8 EU Privacy Directive (updated May 2000)
Information Security Policies
Toolkit & Critical Steps

2. Assigning Roles and Responsibilities

• Managing Information Security Programs
  – CPRI Guide on management processes - 4.4.2
  – Case Study of UPenn electronic registry - 4.4.3
Managing Information Security Programs

4.4.2 CPRI Guidelines for Managing Information Security Programs
4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania
Toolkit & Critical Steps

3. Building Risk Management Capability

- **CPRI Toolkit** - 4.5
  - Health Information Risk Assessment and Management
    - Software Engineering Institute
  - Risk assessment - 4.5.1
  - Risk management plan - 4.5.2
Building
Risk Management
Capability
4. Driving enterprise-wide awareness

- **Information Security Education - 4.6**
  - CPRI Guide on security training - 4.6.1
  - Sample Instructor’s guide and slides - 4.6.2
Information Security Education
Toolkit & Critical Steps

5. Enforcing Security Policies

• Confidentiality Statements - 4.8
  – Harvard Vanguard Policies - 4.3.1
  – Mayo Clinic Policies - 4.3.3
  – Kaiser Reaccreditation Process - 4.8.2
Enforcing Security Policies
Toolkit & Critical Steps

6. Implementing Security Infrastructure

- CPR Guide on Security Features - 4.9.1
- Special Issues in electronic media - 4.9.2
  - Fax, email
  - HCFA Internet Policy
  - Technology for securing the Internet
  - Connecticut Hospital Association PKI
  - Business Continuity Planning & Disaster Recovery Planning - 4.10
Implementing Security Infrastructure
Toolkit & Critical Steps

7. Institutionalizing Responsibility

• Kaiser’s Trustee-Custodian Agreement
Institutionalizing Responsibility
Toolkit & Critical Steps

8. Enhancing Patient Understanding

• Toolkit - Section 4.3.4
  – Partners Healthcare System, Inc.
• Toolkit - Chapter 5.0
  – AHIMA Forms
  – HelpBot - Georgetown University
Enhancing Patient Understanding

5.0 Enhancing Patient Understanding

5.1 Introduction

5.2 Complying with Consent, Inspection, and Disclosure Requirements

5.3 HelpBot: Complying with Patient Education Requirements
Results

Enhanced judgement in managing health information

Improved health care information security
CPRI-HOST Confidentiality and Security Training Video

• What if it were yours?
• Donated to CPRI-HOST by Kaiser Permanente
• www.cpri-host.org
HIPAA Self-evaluation Tools

» Privacy HEVp
» Security HEVs

www.nchica.org
What is HIPAA EarlyView™ Privacy?

A self-assessment software tool for physician practices and others covered by the privacy rule

Developed by:

The Maryland Health Care Commission (MHCC)
The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)
What Does HIPAA EarlyView™ Privacy Do?

• *Organizes* your initiative toward compliance with HIPAA privacy rules

• Provides a *‘gap analysis’* to show what you need to do to comply

• *Clarifies* the HIPAA privacy regulations

• Provides a program of *action* for HIPAA compliance

• Provides *templates* for key HIPAA compliance documents
How Can We Use HIPAA EarlyView™ Privacy?

- *Educate* staff on HIPAA requirements.
- Perform a ‘*gap analysis*’:
  - Identify inadequate or missing policies.
  - Identify unmanaged risks.
- *Document* your organization’s ‘due diligence’ in meeting HIPAA requirements.
- *Manage* preparation of compliance documents.
What is *HIPAA EarlyView™ Security*?

- 1.0 is based on the proposed version of the rules. Version 2.0 will be available for upgrade within two months after the final rule appears.
- HIPAA EarlyView™ Security is intended for health plans, provider organizations, clearinghouses, and public agencies.
- It has been designed to provide an overview of an organization's current status relative to the implementation requirements in the proposed HIPAA Security Regulations.
- Reports generated through the use of this tool may provide useful guidance to an organization in formulating an appropriate response.
How Can We Use HIPAA EarlyView™ Security?

• Staff education
• Gap analysis
  – Inadequate or missing policies
  – Previously unidentified vulnerabilities
• Due diligence documentation
• Budget planning
Greetings

NCHICA

HIPAA EarlyView™

Version 1.0

HIPAA Security Proposed Regulation Self-Evaluation Tool

http://www.nchica.org
919-558-9258

Copyright 2000 NCHICA All Rights Reserved
Main Menu

HIPAA EarlyView™

- Start New Questionnaire
- Update Existing Questionnaire
- Run Reports
- About HIPAA EarlyView(TM)
- Exit

NCHICA

Copyright © 2000 NCHICA
All Rights Reserved
Enter Contact Data

<table>
<thead>
<tr>
<th>Department Name</th>
<th>sample1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>Org</td>
</tr>
<tr>
<td>Division</td>
<td>Div</td>
</tr>
<tr>
<td>Cost Center</td>
<td>CC</td>
</tr>
<tr>
<td>Project Lead</td>
<td>Proj Lead</td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Address1</td>
<td>Addr1</td>
</tr>
<tr>
<td>Address2</td>
<td>Addr2</td>
</tr>
<tr>
<td>City</td>
<td>City</td>
</tr>
<tr>
<td>State</td>
<td>ST</td>
</tr>
<tr>
<td>Zip</td>
<td>99999-9999</td>
</tr>
<tr>
<td>Phone</td>
<td>(999) 999-9999 Ext.</td>
</tr>
<tr>
<td>Fax</td>
<td>(999) 999-9999</td>
</tr>
<tr>
<td>E-Mail</td>
<td><a href="mailto:email@sample.com">email@sample.com</a></td>
</tr>
<tr>
<td>Start Date</td>
<td>1/1/00</td>
</tr>
<tr>
<td>Due Date</td>
<td>12/31/00</td>
</tr>
<tr>
<td>Facilitator</td>
<td>Facilitator</td>
</tr>
<tr>
<td>Title</td>
<td>Title</td>
</tr>
<tr>
<td>F. Phone</td>
<td>(999) 999-9999 Ext.</td>
</tr>
<tr>
<td>F. E-Mail</td>
<td><a href="mailto:facilitator@sample.com">facilitator@sample.com</a></td>
</tr>
<tr>
<td>Serial #</td>
<td>1234</td>
</tr>
</tbody>
</table>
Update Questionnaire Menu

Update Existing HIPPA Questionnaire for sample1

- Continue this Questionnaire
- Update Contact Information
- Return to Main Menu
Security Questions

Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Unanswered</th>
<th>Due Diligence Demonstrated:</th>
<th>Check if YES</th>
</tr>
</thead>
</table>

Comments: evaluation done by test org - June 1999

Periodically Reviewed: No

Document Name: tech eval

Doc Type: Paper

Point of Contact: Mr. Contact

Contact Title: boss

Contact FAX: (999) 999-9999

Answer Date (M/D/Y): 6/9/00

Redress Requirement: Yes

Contact E-Mail: boss@sample.com

Contact Phone: (999) 999-9999 Ext. 1234
Report Menu
## Questions answered with "NO"

<table>
<thead>
<tr>
<th>HIPAA Table</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA Requirement</td>
<td>Certification</td>
</tr>
<tr>
<td>HIPAA Implementation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Detailed Question</th>
<th>Refer To:</th>
<th>Contact</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?</td>
<td>Susan Reference</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HIPAA EarlyView™

target your weaknesses with this powerful self-evaluation tool

Privacy
$350 per site
($100 per site for NCHICA members)

Security
$150 per site
($50 per site for NCHICA members)

www.nchica.org
Managing Information Security in Healthcare

ISO/IEC 17799:2000
Information technology — Code of practice for information security management

- http://www.iso17799software.com/
What is information security?

Information security is characterized as the preservation of:

• Confidentiality: ensuring that information is accessible only to those authorized to have access;

• Integrity: safeguarding the accuracy and completeness of information and processing methods;

• Availability: ensuring that authorized users have access to information and associated assets when required.
How is information security achieved?

• By implementing a set of controls:
  – policies
  – practices
  – procedures
  – organizational structures
  – software functions

• These controls need to be established to ensure that the specific security objectives of the organization are met.
Source of security requirements

- Assess risks to the organization
  - threats to assets
  - vulnerabilities
  - likelihood of occurrence
  - impact
- Legal, statutory, regulatory and contractual requirements
  - requirements
  - trading partners
  - contractors
  - service providers
- Information processing to support operations
  - principles
  - objective
  - requirements
Risk Assessment Life Cycle

It is important to carry out periodic reviews of security risks and implemented controls to:

• take account of changes to business requirements and priorities;
• consider new threats and vulnerabilities;
• confirm that controls remain effective and appropriate.
Controls

Expenditure on controls needs to be balanced against the business harm likely to result from security failures.
ISO/IEC 17799 Areas to Address

- Information Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical & Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development & Maintenance
- Business Continuity Management
- Compliance

- All of HIPAA Security Is Covered
CERT® Coordination Center (CERT/CC), a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
http://www.cert.org/nav/index.html

- CERT® Security Improvement Modules
  http://www.cert.org/security-improvement/#modules
Information Security Risk Assessments: A New Approach

• Christopher Alberts
• Team Leader
  – Security Risk Assessments

• Software Engineering Institute
• Carnegie Mellon University
• Pittsburgh, PA 15213

• Sponsored by the U.S. Department of Defense
  (Will be used by military treatment facilities)
OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation is an approach for self-directed risk evaluations that

- puts organizations in charge
- balances critical information assets, business needs, threats, and vulnerabilities
- measures the organization against known or accepted good security practices
Self-Directed IS Risk Assessments

• Goals:
  – To enable organizations to direct and manage risk assessments for themselves
  – To enable organizations to make the best decisions based on their unique risks
  – To focus organizations on protecting key information assets
Why a Self Directed Approach?

• SEI’s experience
  – Acting as external resource
    • Identify specific problems
    • Provide “laundry list” of items to be fixed
    • Fixes applied by organization
    • Next assessment similar issues identifies
    • Root cause of issues remains
Why a Self Directed Approach?

• SEI’s experience
  – Sees need for organizations to internalize risk assessment
    • approach
    • education/knowledge
    • practices
    • instill a change in culture
Benefits

• Organizations will identify information security risks that could prevent them from achieving their missions.
• Organizations will learn to direct information security risk assessments for themselves.
• Organizations will identify approaches for managing their information security risks.
• Medical organizations will be better positioned to comply with HIPAA requirements.
IS Risk Assessment

- Organizational View
- Technology View

Risk Analysis
OCTAVE

• Overview
  – http://www.cert.org/octave/
  – http://www.cert.org/octave/omig.html
  – http://www.cert.org/octave/methodintro.html

Version 2.0 on-line

• Printed guide & the CD-ROM is $400
Generally Accepted System Security Principles (GASSP)

• The International Information Security Foundation (I²SF) - Sponsored Committee to Develop and Promulgate Generally Accepted System Security Principles
  
• http://web.mit.edu/security/www/gassp1.html
SANS Institute
System Administration, Networking, and Security

• The Twenty Most Critical Internet Security Vulnerabilities the Experts’ Consensus

• How to Eliminate the Ten Most Critical Internet Security Threats the Experts’ Consensus
  – http://www.sans.org/topten.htm

• Model Policies
  – http://www.sans.org/newlook/resources/policies/policies.htm
WEDI SNIP

• **Strategic National Implementation Process** for Complying with the Administrative Simplification Provisions of the Health Insurance

• **Vision**

SNIP is a collaborative healthcare industry-wide process resulting in the implementation of standards and furthering the development and implementation of future standards.
WEDI SNIP Mission

The WEDI HIPAA SNIP Task Group has been established to meet the immediate need to assess industry-wide HIPAA Administrative Simplification implementation readiness and to bring about the national coordination necessary for successful compliance.

• SNIP is a forum for coordinating the necessary dialog among industry implementers of the HIPAA standards.

• SNIP will identify industry "best practices" for implementation of HIPAA standards.

• SNIP will identify coordination issues leading toward their resolution as industry adopted "best practices."

• SNIP will adopt a process that includes an outreach to current industry initiatives, an information gap analysis, and recommendations on additional initiatives to gap-fill.
WEDI SNIP Purpose

• Promote general healthcare industry readiness to implement the HIPAA standards.

• Identify education and general awareness opportunities for the healthcare industry to utilize.

• Recommend an implementation time frame for each component of HIPAA for each stakeholder [Health Plan, Provider, Clearinghouse, Vendor] and identify the best migration paths for trading partners.

• Establish opportunities for collaboration, compile industry input, and document the industry "best practices."

• Identify resolution or next steps where there are interpretation issues or ambiguities within HIPAA Administrative Simplification standards and rules.

• Serve as a resource for the healthcare industry when resolving issues arising from HIPAA implementation.
WEDI SNIP Products

- WEDI SNIP Webcasts
- Transactions White Papers
- Security & Privacy White Papers
- Conference Presentations
- Discussion Forum
- HIPAA Issues Database
- Surveys

http://www.wedi.org
Academic Medical Centers HIPAA Privacy & Security Guidelines

• Association of American Medical Colleges
• GASP
  – Guidelines for Academic Medical Centers on Security and Privacy: *Practical Strategies for Addressing the Health Insurance Portability and Accountability*
  – amc-hipaa.org
AAMC HIPAA Privacy & Security Guideline Sponsors

• Association of American Medical Centers
• Internet 2
• National Library of Medicine
• Object Management Group
AAMC HIPAA Privacy & Security
Supporting Organizations

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

- Privacy & Security Regulations
- AAMC explanation of each regulation
- What you must do
- What you should do
- Organizing principles
Guidelines for Academic Medical Centers on Security and Privacy

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

Contact for questions and ordering information

(links below are all pdf files)

Table of Contents

Background
  Executive Summary (file size 266kb)  
  Introduction  
  Purpose, Scope and Acknowledgments  
  AMC Guidelines Organization of the Guidelines  

AMC HIPAA Security Guidelines  
  Section One: Requirements for Security Administration  
  Section Two: Requirements for Physical Safeguards  
  Section Three: Requirements for Technical Security, Services, and Mechanisms  

AMC HIPAA Privacy Guidelines  
  Section One: Covered Entities  
  Section Two: Content and Authorization  
  Section Three: Uses and Disclosures  
  Section Four: Consumer Controls  
  Section Five: Administrative requirements AMC  

AMC General Policy and Management Guidelines  

Acronyms  
Definitions of Terms Used in this Guidelines  
References  

The privacy and security regulations stemming from the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have captured the attention of the healthcare community. The cumulative cost of compliance with these regulations is variously estimated to cost from somewhere between the equivalent of Y2K preparation for the community to many times that amount. A recent study commissioned by the American Hospital Association placed costs at $22.5 billion over the next five years. To assist medical schools and teaching hospitals in addressing the new regulations, The National Library of Medicine (NLM) funded a series of workshops engaging the membership of several organizations: AAMC's Group on Information Resources, Internet2, Object Management Group, and Workgroup on Electronic Data Interchange. The workshop participants analyzed current health information security and privacy policies, made recommendations, and developed this resource of best practices for healthcare security and privacy. The Guidelines for Academic Medical Centers on Security and Privacy: Practical Strategies for Addressing the Health Insurance Portability and Accountability Act (HIPAA) addresses the unique concerns of academic medical centers.

The traditional tripartite mission - patient care, education, and research - distinguishes academic medical centers (AMC) from their peer institutions, which focus primarily on patient care services. In the past two decades the ability of academic medical centers to balance and sustain these multiple missions has been severely tested by changes in health care financing and regulation. The implementation of the HIPAA regulations will create barriers unique to these environments. Because of their multiple missions and collegial concerns, AMCs have come together in an effort to create the guidelines - to ensure the privacy, security and confidentiality of patient information.
PSN HI PAA Calculators™

- The PSN HI PAA Calculators™ provide you with free - real-time - initial consultations of your organization's compliance with the HI PAA data, security and privacy requirements.

- You will be guided through a series of questions about your organization and its practices. Based upon your answers, the HI PAA Calculator™ will generate a report that identifies areas that your organization may want to address.

- If you do not understand any question, you may answer "Do Not Know," and the HI PAA Calculator™ will take that answer into account when preparing the Report.

- http://www.privacysecuritynetwork.com/healthcare/hipaa/
Thank you!