

The CPRI Toolkit: Managing Information Security in Health Care And other HIPAA Tools

Jeff Collmann, PhD
Associate Professor
Department of Radiology
Georgetown University

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.**

HIPAA Standards for Security & Privacy

- **Was not issued in August**
- **When will they be issued?**
 - **Rumors**
 - **Guesses**
- **When do the final rules become effective?**

Tools

- ***CPRIToolkit: Managing Information Security in Health Care***
- ***NCHICA's HIPAA EarlyViewTM***
- ***SEI's Self Risk Assessment Tool***
- ***WEDI's HIPAA Security Summit Implementation Guidelines***

The CPRI Toolkit: Managing Information Security in Health Care

- **How to use it to address HIPAA confidentiality and security**

CPRI Toolkit

Original Task Force 1998

- **Ted Cooper, MD - task force chair**
- **Jeff Collmann, PhD - editor**
- **Barbara Demster, MS, RRA**
- **Keith MacDonald**
- **Susan K. Odneal, CISSP**
- **Jeanne Reiners**

CPRI Toolkit

Content Committee 2000

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

CPRI Toolkit

- **Third Version of *Toolkit* - May 2000**
- **<http://www.cpri-host.org>**

Goal

**Build
security capable
organizations!**

Goal

**Incorporate sound security practices
in the everyday work of all members of
the organization, including the patient.**

NOT JUST

Implementing 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

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

3Com® Buy Direct Enterprise United States

Products Service & Support Contact us Site Map Countries

Search Review Cart

Advanced Search

3COM HEALTHCARE HOME

SECURITY NET

HIPAA e-SOURCE

3COM SECURITY SOLUTIONS

TECHNICAL RESOURCE CENTER

TRAINING OPPORTUNITIES

RELATED LINKS

CPRI CONTENT COMMITTEE

Robert Pennington
Ted Cooper, MD
Task Force Chair
National Director of
Confidentiality and
Security

Georgetown University Medical Center
Jeff Collman, Ph.D.,
Editor, Department
of Radiology

CPRI Toolkit
Computer-based Patient Record Institute

CPRI Toolkit: Managing Information Security in Health Care, Version 2

[HTML Table of Contents](#) [Learn more about CPRI](#)

Get Acrobat Reader [Document Download Center](#)

[1.0 Executive Summary](#)

[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/Code Sets

[3.2.5](#) Health Care Provider Identifier

Download Center

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Document Download Center - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

• [Advanced Search](#)

3COM HEALTHCARE HOME

SECURITY NET


• **HIPAA e-SOURCE**

3COM SECURITY SOLUTIONS

TECHNICAL RESOURCE CENTER

TRAINING OPPORTUNITIES

RELATED LINKS


CPRI Toolkit 

Document Download Center

CPRI Toolkit: Managing Information Security in Health Care, Version 2

[PDF Table of Contents](#) [Back to HTML Table of Contents](#)

The Document Download Center has been provided for your printing convenience. In order to download the PDF files you will need to download the Adobe Acrobat Reader. A link to the Acrobat Reader has been provided below.



[CPRI Toolkit by sections](#) [Entire CPRI Toolkit \(1.8MB, Apx.505pp\)](#)

CPRI CONTENT COMMITTEE

Falser Pennington
Ted Cooper, MD
Task Force Chair
National Director of Confidentiality and Security

Georgetown University Medical Center
Jeff Colman, Ph.D.,
Editor
Department of Radiology

AHIMA
John Lee Frawley, J.D.
Legislative and Policy Department

DHHS
John Fanning
Privacy Advocate

HCFA
John Fanning

1.0 Executive Summary

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/Code 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](#)

Toolkit - Sections 1 & 2

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links >>

3Com®

Buy Direct

Enterprise
United States

Products Service & Support Contact us Site Map Countries

Search Review Cart

Advanced Search

3COM HEALTHCARE HOME

SECURITY NET

HIPAA e-SOURCE

3COM SECURITY SOLUTIONS

TECHNICAL RESOURCE CENTER

TRAINING OPPORTUNITIES

RELATED LINKS

CPRI CONTENT COMMITTEE

Kaiser Permanente

Ted Cooper, MD
Task Force Chair
National Director of Confidentiality and Security

CPRI Toolkit
Computer-based Patient Record Institute

CPRI Toolkit: Managing Information Security in Health Care, Version 2

HTML Table of Contents Learn more about CPRI

Get Acrobat Reader Document Download Center

1.0 Executive Summary

2.0 Introduction

2.1 How to Use This Toolkit

3.0 Monitoring Laws, Regulations, and Standards

3.1 Introduction

Toolkit - Section 3

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet E...

File Edit View Favorites Tools Help Links >>

| | |
|---|---|
| National Director of Confidentiality and Security | <u>3.0</u> Monitoring Laws, Regulations, and Standards |
| | <u>3.1</u> Introduction |
| | <u>3.2</u> Summary of Proposed DHHS Rules |
| | <u>3.2.2</u> Common Elements |
| | <u>3.2.3</u> Proposed Data Security and Electronic Signature Standards |
| | <u>3.2.4</u> Electronic Transactions/Code Sets |
| | <u>3.2.5</u> Health Care Provider Identifier |
| | <u>3.2.6</u> Employer Identifier |
| | <u>3.2.7</u> Health Plan Identifier |
| | <u>3.2.8</u> Unique Health Identifier - Individuals |
| | <u>3.3</u> Final Federal HIPAA Security & Electronic Signature Standard |
| | <u>3.4</u> Federal Medical Privacy Legislation |
| | <u>3.4.1</u> Summary of DHHS Confidentiality Recommendations |
| | <u>3.4.2</u> Privacy Notice of Proposed Rule Making |
| | <u>3.5</u> State Medical Privacy Legislation |
| | <u>3.6</u> Setting Standards in Health Care Information (12/15/1999) |
| | <u>3.7</u> JCAHO/NCQA Recommendations for Protecting Personal Health Information |
| | <u>4.0</u> Developing Policy, Procedures, and Practices |

George Washington University Medical Center
Jeff Collman, Ph.D.,
Editor, Department of Radiology

AHIMA
Harry Rhodes, MBA,
RHIA, Director of HIM Products and Services

Catholic Healthcare East
Jack Heiter
VP and CIO

DHHS
John Fanning
Privacy Advocate

HCFA
John Pampliani

Toolkit - Section 4.0 - 4.5.2

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links >>

| | |
|---|--|
| Director Enterprise Standards | 4.0 Developing Policies, Procedures, and Practices |
| | 4.1 Introduction |
| HCFA | 4.2 CPRI Guidelines - Information Security Policies |
| Barbara Clark Senior Systems Analyst | 4.3 Sample Security Policies |
| | 4.3.1 Harvard Vanguard Medical Associates |
| JCAHO | 4.3.2 Kaiser Permanente Northern California |
| Paul Schyve, MD | 4.3.3 Mayo Clinic |
| | 4.3.4 Partners Healthcare System |
| 3Com Corporation | 4.3.5 PCASSO Security Policy Model |
| Bill Sherman Content Manager, 3Com Security Net | 4.3.6 Project Phoenix, Georgetown University |
| | 4.4 Assigning Roles and Responsibilities |
| | 4.4.1 Introduction |
| Healtheon/WebMD | 4.4.2 CPRI Guidelines for Managing Information Security Programs |
| Barbara Demster, MS, RHIA, Compliance Officer | 4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania |
| IBM | 4.5 Conducting Data Security Risk Analyses |
| Shannah Koss Healthcare Security and Government Programs Executive | 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 - 4.9.3

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links »

- [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 (**Online View**)
 - [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)

Toolkit - Section 5-9

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links »

- [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**

[Login](#) | [Solutions & Technologies](#) | [Training & Seminars](#) | [Corporate Information](#) | [Legal](#)

[Home](#) | [Buy Direct](#) | [Products](#) | [Service & Support](#) | [Contact Us](#) | [Site Map](#) | [Countries](#) | [Site Search](#)
[Log In](#) | [Solutions & Technologies](#) | [Training & Seminars](#) | [Corporate Information](#) | [Legal](#) | [Privacy Statement](#)
[Copyright © 1999 3Com Corporation. All rights reserved.](#)

Managing Information Security in Health Care

- **Policy = what you want done**
- **Procedure = how it should be done**
- **Technology used to enforce policies & procedures through automation**
- **Practice = what is done - audit**

Requires a Plan

- **The plan should address all four**

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: 2002-2003

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**
 - Data Security Rules - 3.1
 - Federal Medical Privacy - 3.2
- **State Medical Privacy Laws - 3.3**
- **Setting Standards - 3.4**
- **JCAHO/NCQA Recommendations - 3.5**
- **New: EU Privacy Directive - “Safeharbor”**

Toolkit - Section 3

3Com | Security Net | HIPAA e-Source | CPRI Toolkit Table of Contents - Microsoft Internet E...
File Edit View Favorites Tools Help Links >>

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/Code 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

4.0 Developing Policies, Procedures, and Practices

National Director of Confidentiality and Security

Georgetown University Medical Center
Jeff Collman, Ph.D.,
Editor, Department of Radiology

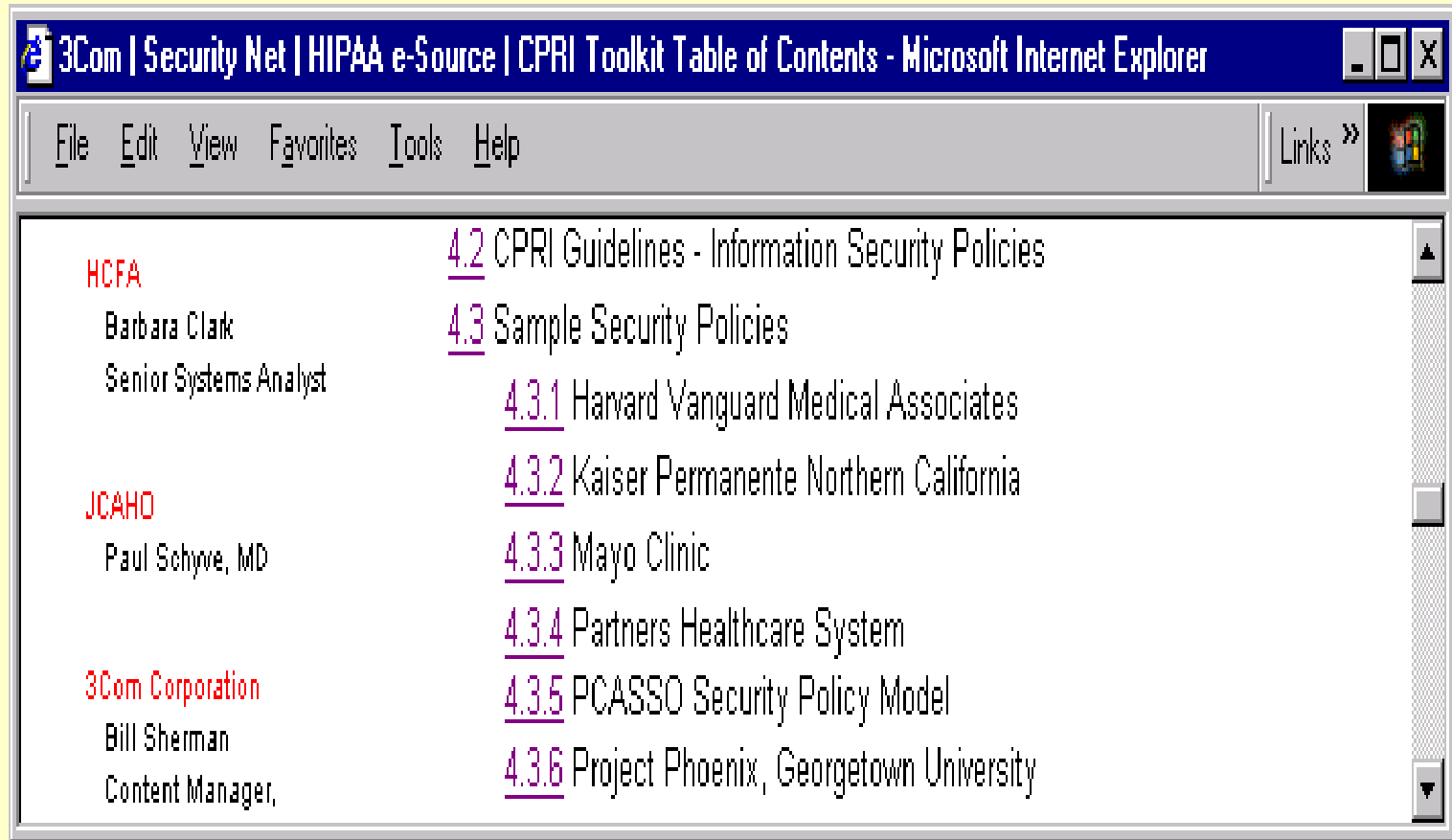
AHIMA
Harry Rhodes, MBA,
RHIA, Director of HIM Products and Services

Catholic Healthcare East
Jack Heiter
VP and CIO

DHHS
John Fanning
Privacy Advocate

HCFA
John Pampliani

Information Security Policies

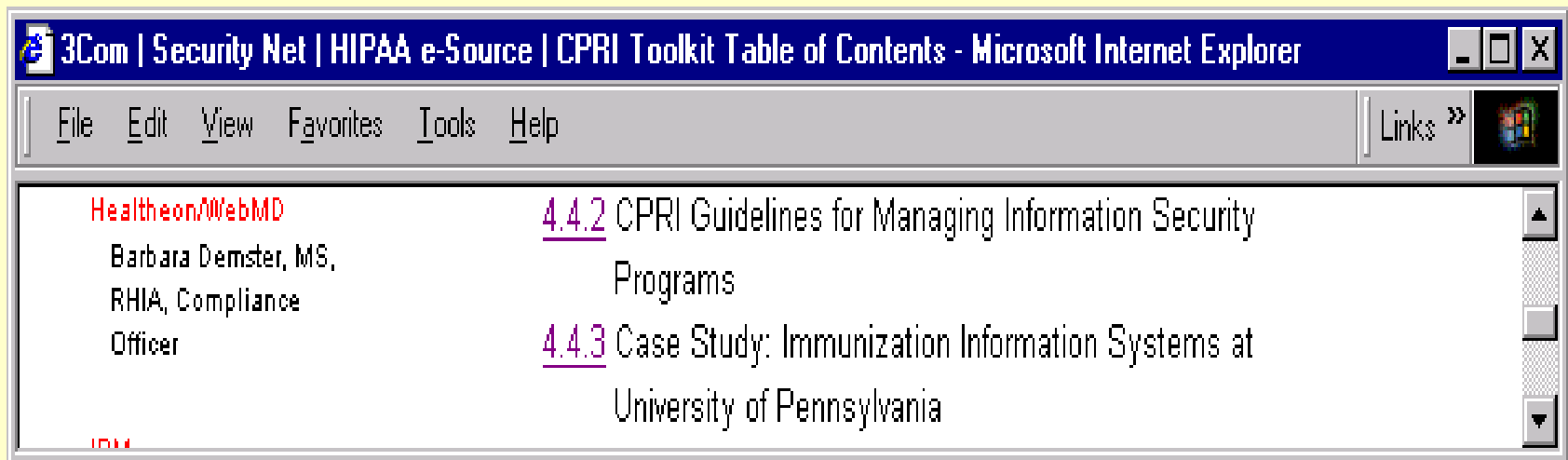


Toolkit & Critical Steps

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

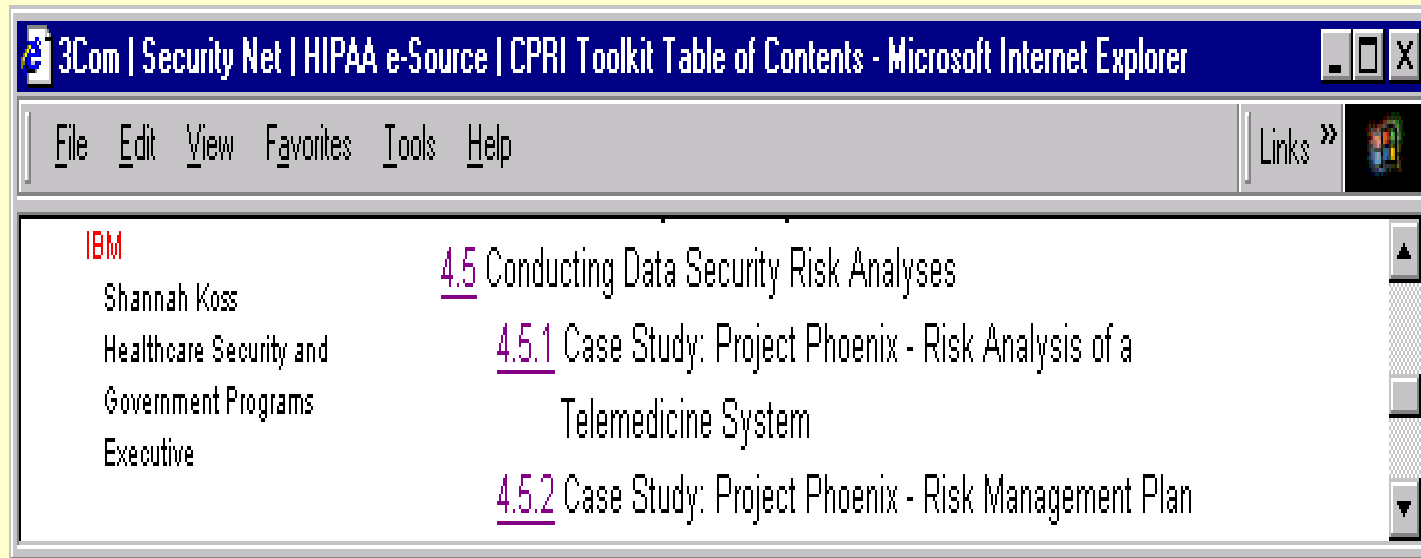


Toolkit & Critical Steps

3. Building Risk Management Capability

- ***CPRI Toolkit - 4.5***
 - **New Health Information Risk Assessment and Management**
 - **Software Engineering Institute**
 - **Risk assessment - 4.5.1**
 - **Risk management plan - 4.5.2**

Building Risk Management Capability

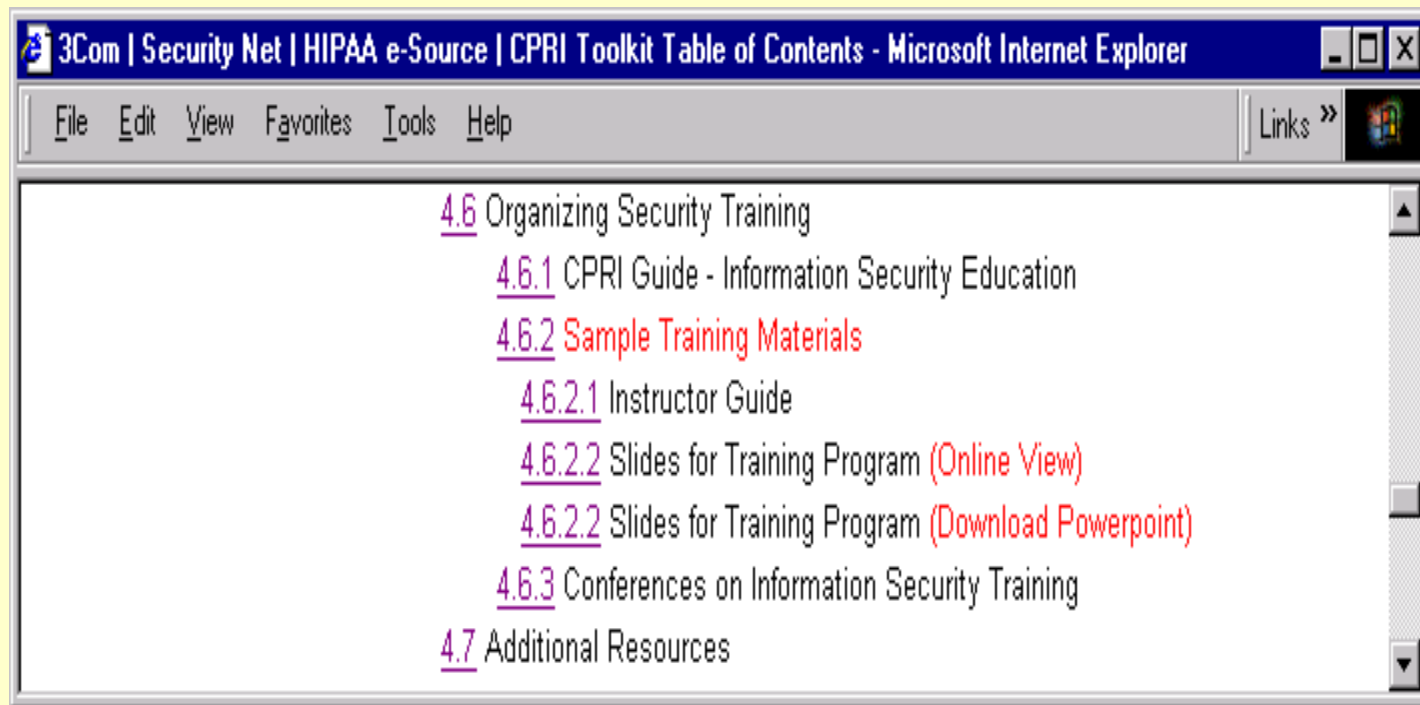


Toolkit & Critical Steps

4. Driving enterprise-wide awareness

- ***Information Security Education - 4.6.1***
 - **CPRI Guide on security training**
 - **Sample Instructor's guide and slides - 4.6.2**

Information Security Education

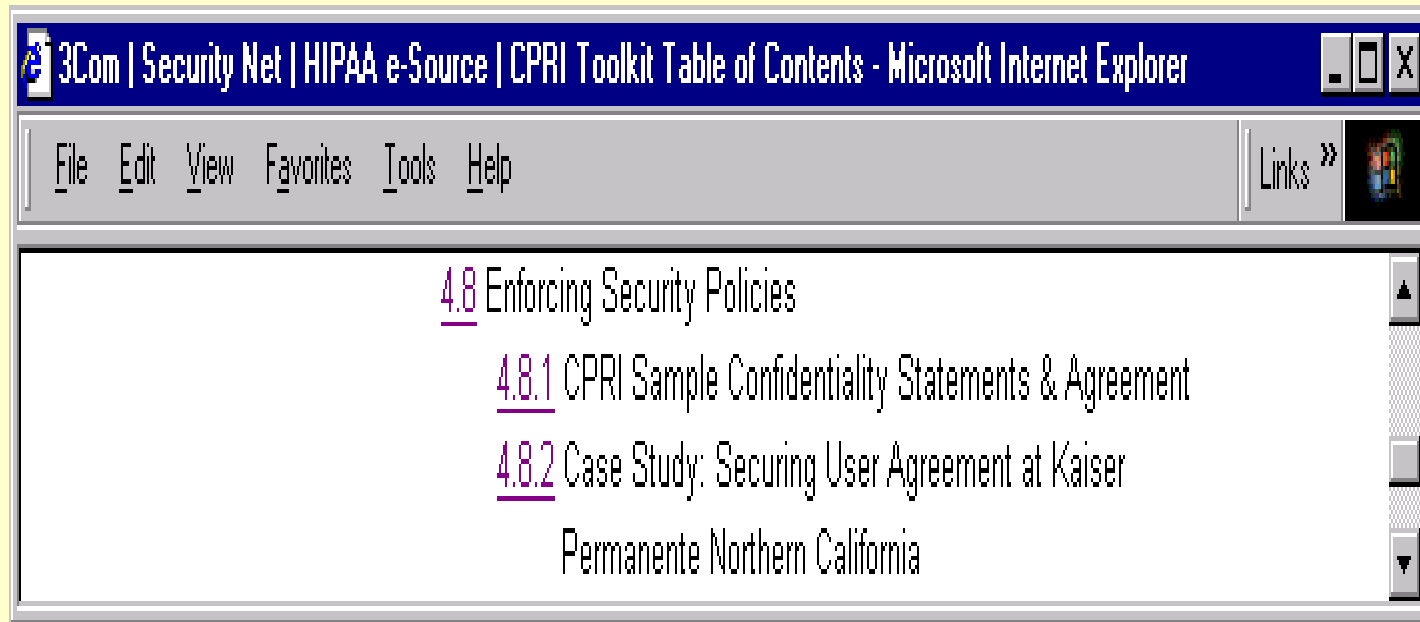


Toolkit & Critical Steps

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

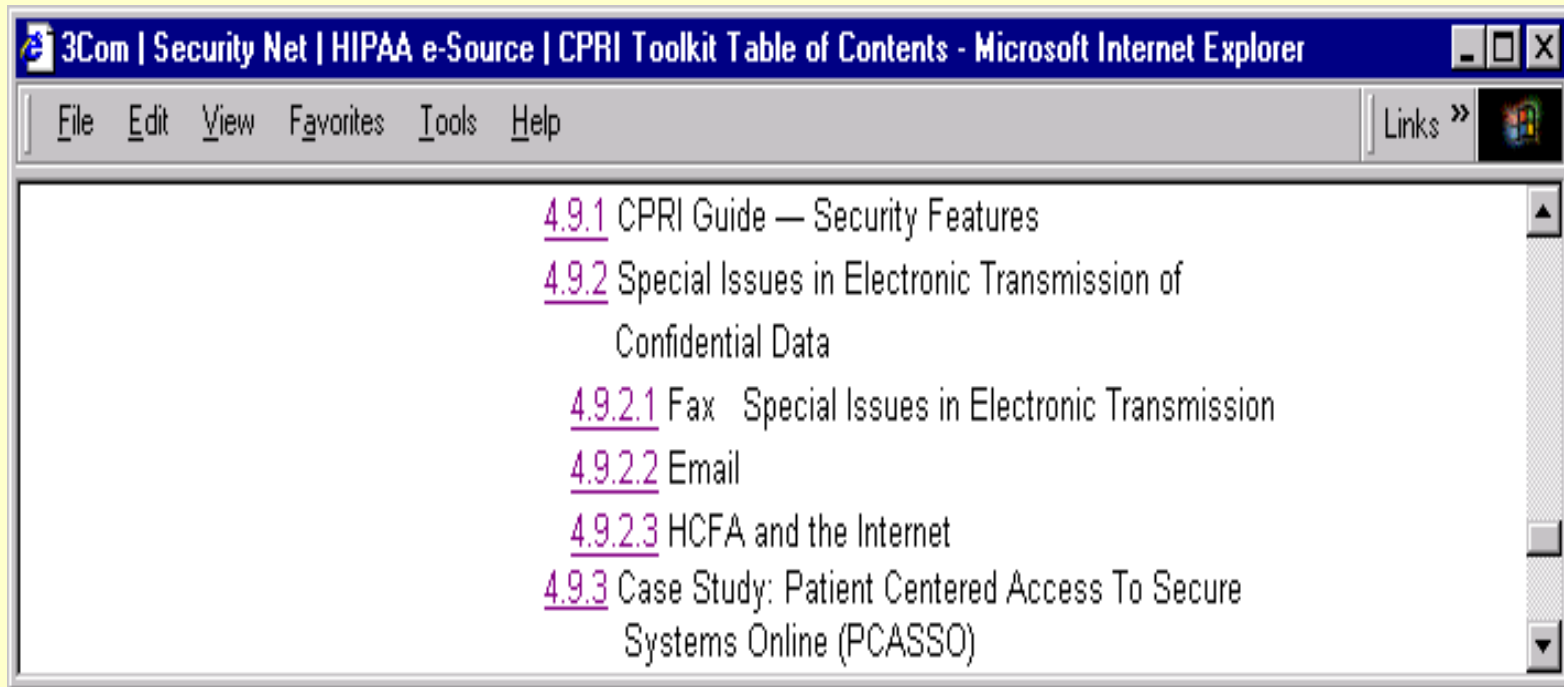


Toolkit & Critical Steps

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
 - **New:** Connecticut Hospital Association PKI
 - **New:** Business Continuity Planning & Disaster Recovery Planning - 4.10

Implementing Security Infrastructure

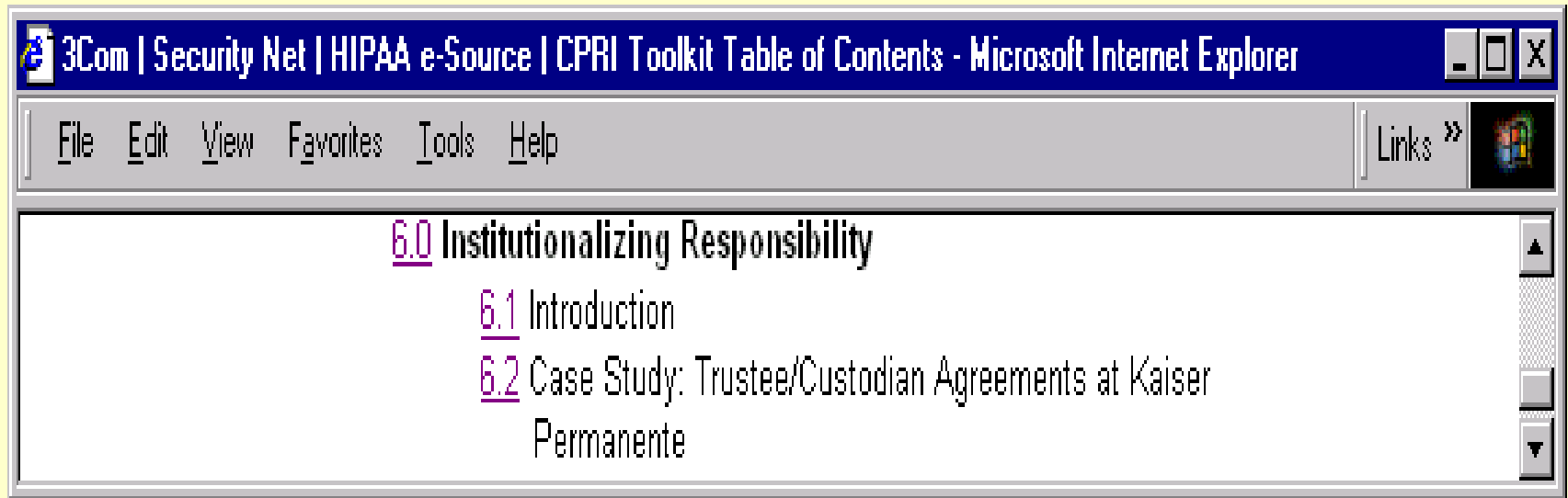


Toolkit & Critical Steps

7. Institutionalizing Responsibility

- **Kaiser's Trustee-Custodian Agreement**

Institutionalizing Responsibility

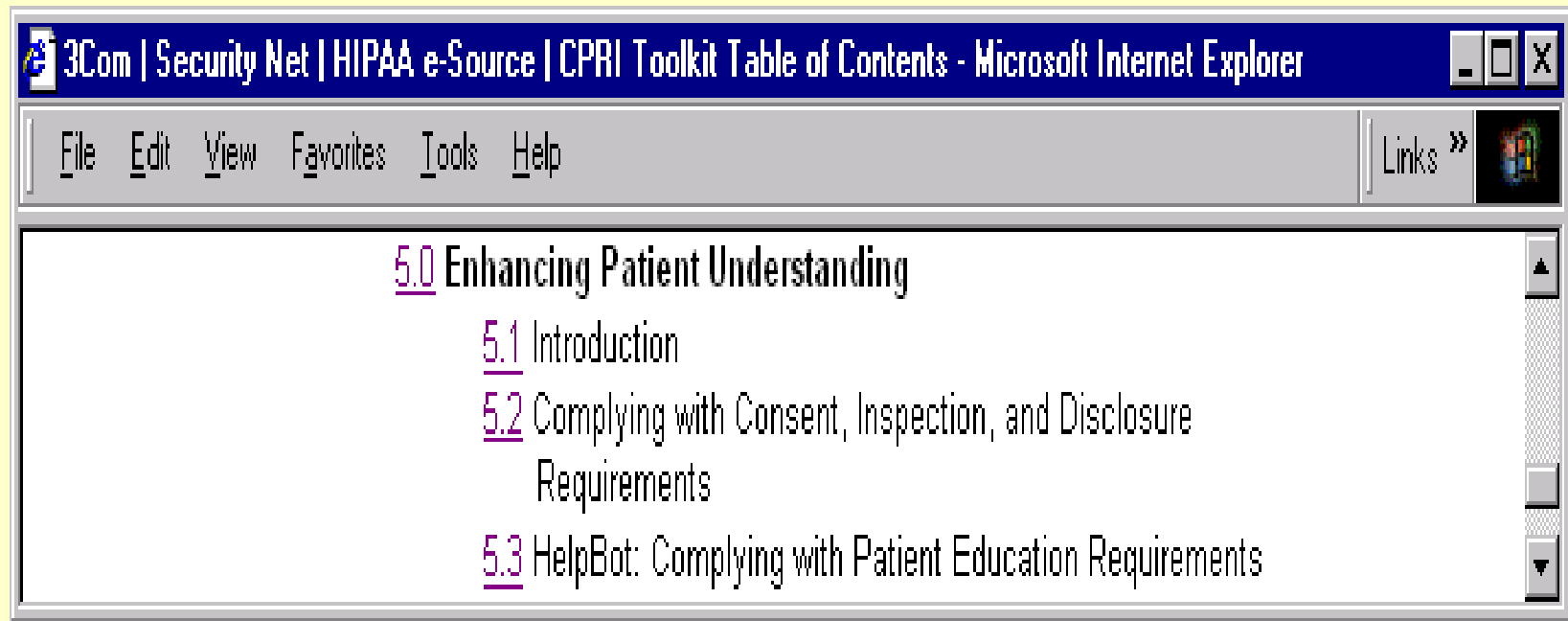


Toolkit & Critical Steps

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



Results

Enhanced judgement
in managing health information

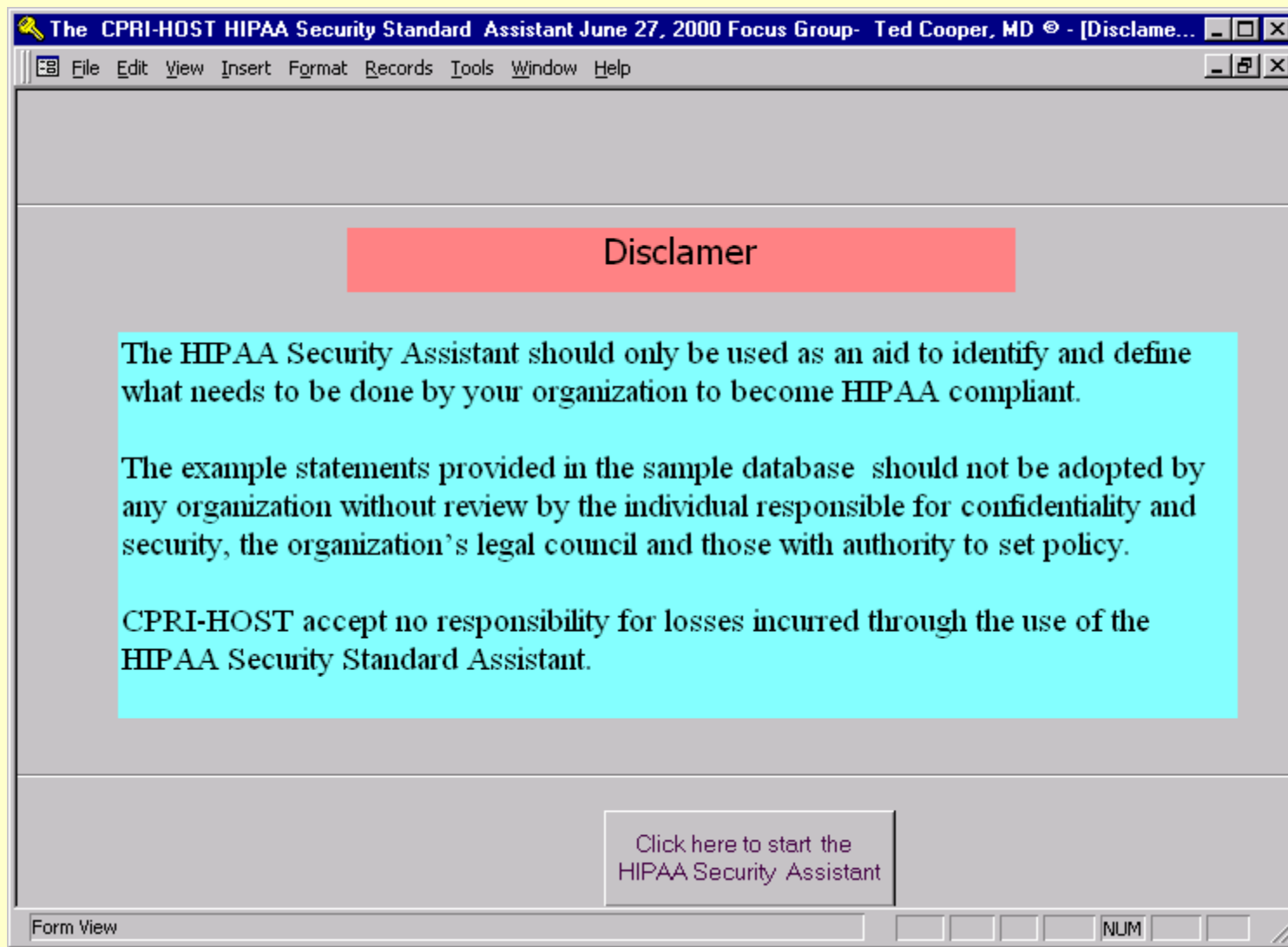
Improved health care information security

HIPAA Security Assistant

- **Microsoft Access Database Application**
- **Displays each HIPAA Security**
 - Requirement & Implementation Feature
 - One at a time
- **Provides for your entry of**
 - Items needed to be done to address each
 - A description of each item

HIPAA Security Assistant

- **Future CPRI-HOST Product**
- **Focus Groups are being conducted**
 - **Contribute Content**
- **Analysis will be done to determine which items are common**
- **Can provide output in**
 - **MS Access Reports**
 - **MS Word file**
 - **MS Excel file**



HIPAA Category **Administrative Procedure**
 Requirement
 Certification

HIPAA Number **142.308.a.1**
 Implementation Feature
 None

(1)The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.

For each requirement implementation feature enter the concept for each item to be addressed in this column.

Enter what should be done to respond to this item in this column.

| Concept | Description of What Needs to Be Done |
|---|--|
| Certification method | To perform the certification method to evaluate software, databases and networks is needed. |
| Authority for performing the technical assessment | The individual who is responsible for performing the technical assessment for certification must be explicitly stated. |
| Authority for accepting residual risk | The corporate officer responsible for accepting any residual risk for systems or networks which do not completely meet the set of certification requirements. |
| Level of software risk | Each software application and reporting database containing patient identifiable information will be classified for level of risk of unauthorized use or disclosure. |
| Level of network risk | Each computer network will be classified for level of risk of unauthorized disclosure. |
| Periodically | Each software application and network will be recertified no less than every 3 years. |
| Before implementing a system or connecting to a new network | A certification evaluation will be performed before connecting any software application or additional network to the Kaiser Permanente network. |
| When system is changed | A certification update will be performed with each release of an application. |
| Inventory of software and networks | An up to date inventory of all software applications, reporting databases and networks will be maintained. |



HIPAA Proposed Security Regulation Self-evaluation Tool

NCHICA

www.nchica.org

Uses of *HIPAA EarlyView*TM

- **Staff education**
- **Gap analysis**
 - **Inadequate or missing policies**
 - **Previously unidentified vulnerabilities**
- **Due diligence documentation**
- **Budget planning**

Greeting



NCHICA

HIPAA EarlyViewTM

Version 1.0

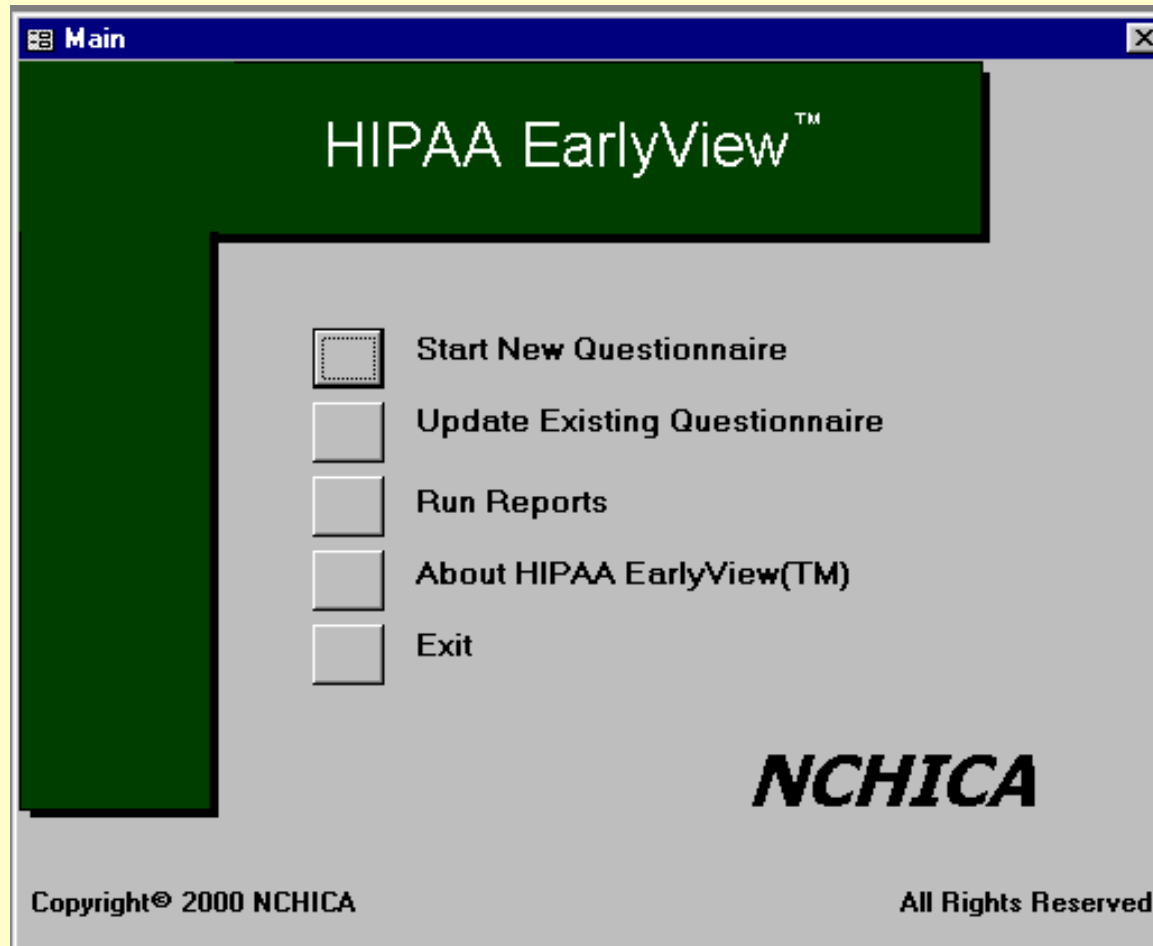
HIPAA Security Proposed Regulation Self-Evaluation Tool

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



Copyright 2000 NCHICA All Rights Reserved

Main Menu



Enter Contact Data

Contact Information Form

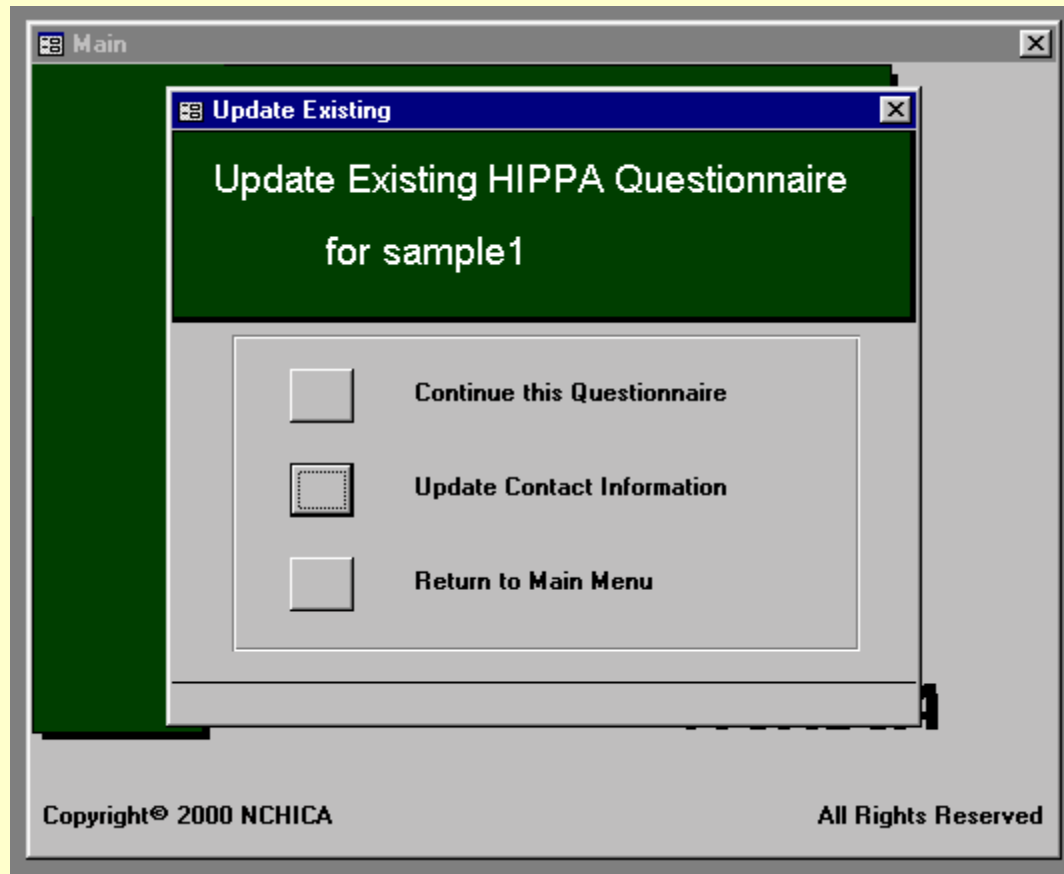
HIPAA Security Questionnaire Contact Data

Department Name

| | | | |
|--------------|--|-------------|---|
| Organization | <input type="text" value="Org"/> | | |
| Division | <input type="text" value="Div"/> | | |
| Cost Center | <input type="text" value="CC"/> | | |
| Project Lead | <input type="text" value="Proj Lead"/> | | |
| Title | <input type="text" value="Title"/> | Start Date | <input type="text" value="1/1/00"/> M/D/YY |
| Address1 | <input type="text" value="Addr1"/> | Due Date | <input type="text" value="12/31/00"/> M/D/YY |
| Address2 | <input type="text" value="Addr2"/> | Facilitator | <input type="text" value="Facilitator"/> |
| City | <input type="text" value="City"/> | Title | <input type="text" value="Title"/> |
| State | <input type="text" value="ST"/> | F. Phone | <input type="text" value="(999) 999-9999 Ext."/> |
| | | F. E-Mail | <input type="text" value="facilitator@sampel.com"/> |
| Phone | <input type="text" value="(999) 999-9999 Ext."/> | Zip | <input type="text" value="99999-9999"/> |
| | | Fax | <input type="text" value="(999) 999-9999"/> |
| E-Mail | <input type="text" value="email@sample.com"/> | Serial # | <input type="text" value="1234"/> |

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved

Update Questionnaire Menu



Security Questions

This form is used by a facilitator to conduct the HIPAA Security Questionnaire. It is designed to be used to capture all required information. Comments should be forwarded to DataSecurity@NCHICA.ORG. Thanks!

Question **1**

Questionnaire Name: sample1

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

Answer: Yes No N/A Unanswered

Due Diligence Demonstrated: Check if YES

Comments: evaluation done by test org - june 1999

Refer To:

Document Name: tech eval

Doc Type: Paper Document Location:

Periodically Reviewed? No Next Review Date (MM/DD/YYYY):

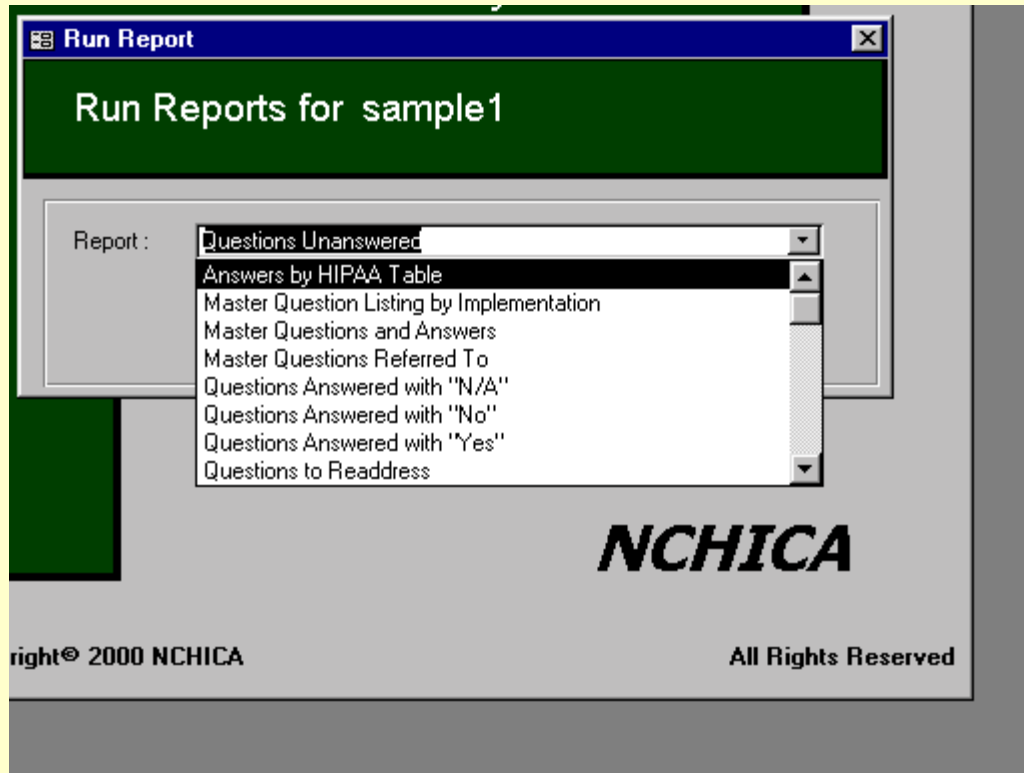
Point of Contact: Mr. Contact Contact Phone: (999) 999-9999 Ext. 1234

Contact Title: boss Contact E-Mail: boss@sample.com

Contact FAX: (999) 999-9999

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

Report Menu



Report Example

Questions answered with "NO"

sample1

HIPAA Table

A

HIPAA Requirement Certification

HIPAA Implementation

| Question Number | Detailed Question | Refer To: | Contact | Contact Phone |
|-----------------|---|-----------------|---------|---------------|
| 2 | Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards? | Susan Reference | | |



Available on the NCHICA Web site:

\$150 license fee per site

(\$50 per site for NCHICA members)

www.nchica.org



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**



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 identified
 - Root cause of issues remained



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.**

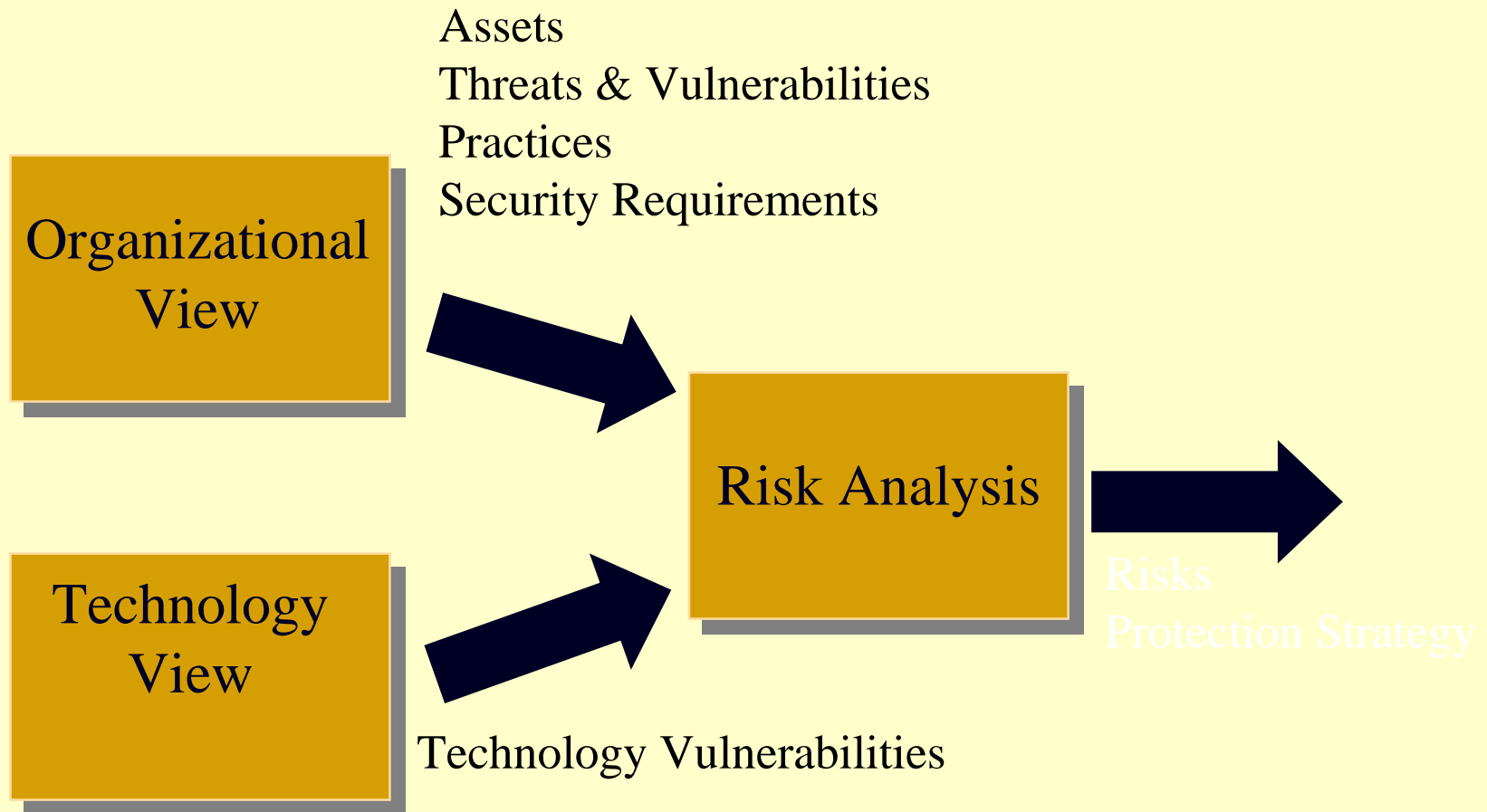


SEI's Self Risk Assessment

- **Aimed at moderate to large sized organizations**
- **Methodology**
- **Team**
- **Workshops**
 - **Senior Management, Middle Management, Staff**
 - **Structured process**
 - **Catalogue of specific references**
 - **Outcome - choices support mission**

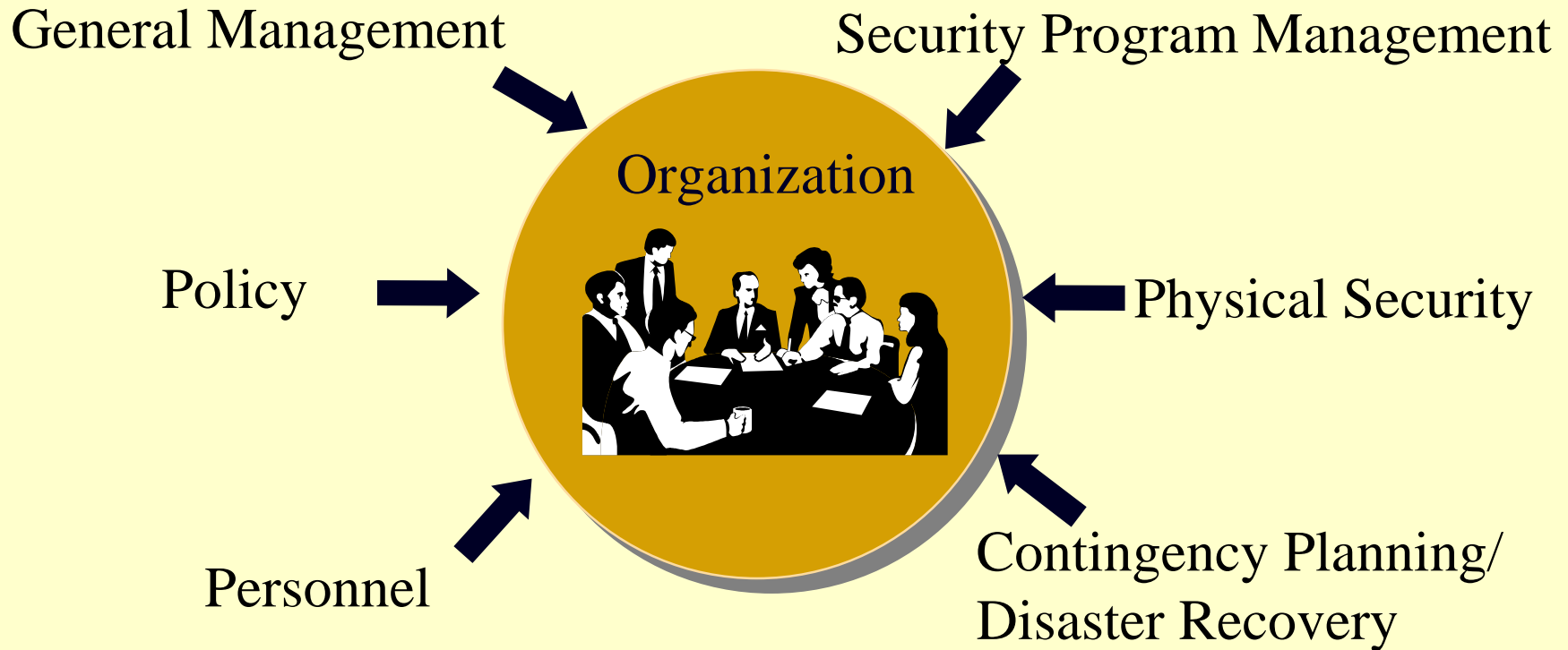


IS Risk Assessment



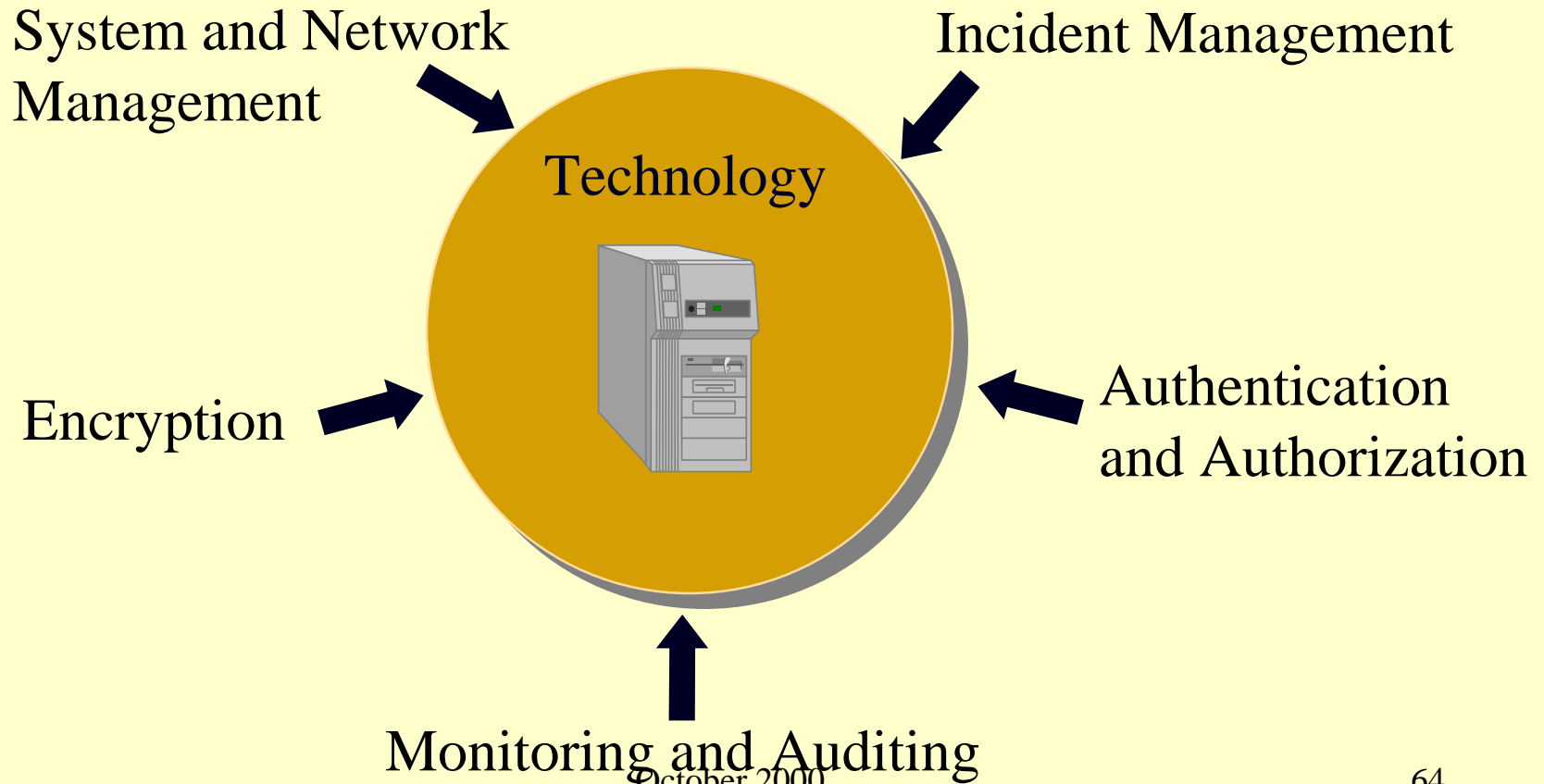


Management Practice Categories



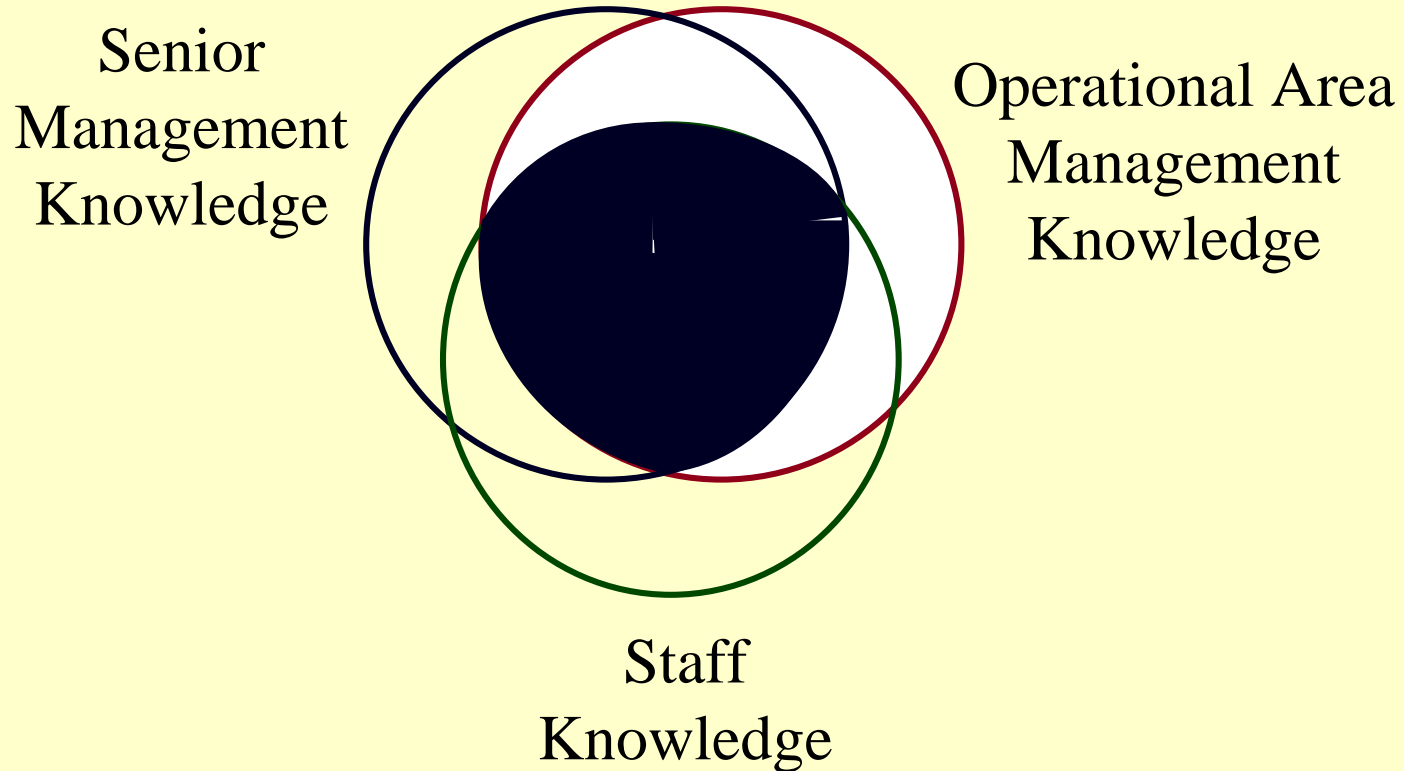


Technology Practice Categories





Distributed Knowledge





SEI Risk Assessment Resource

- **Will be available freely over the Web**
- **Derivative products encouraged**
- **SEI will provide training courses**
- **Will have been validated in field**
- **Expected to be available 6-12 months**

HIPAA Security Summit Implementation Guidelines

Roger May

Support

- **Johns Hopkins**
- **WEDI / Jim Schuping and Steve Lazarus**
- **Track Leaders**
- **Executive Committee**
- **Sponsors**
 - **IBM, TRW, COMPAQ, KSM Healthcare Resources, Johns Hopkins, Microsoft, SMS**
- **Attendees**

What Kind of Guidance?

- **Reasonable**
 - Can you live with it? Does it protect enough?
- **“Implementable”**
 - Can you put it into operation? Keep it there?
- **Scalable**
 - Dentists to Integrated Delivery Systems
- **Business Oriented**
 - How Do I it fit within my Business Processes?
- **Where to Start???**

Partners....

- **CPRI**
- **D.O.D. Rainbow Series**
- **ASC X12N**
- **Consulting and Technology Firms**
 - **Best Practices**
 - **Other Industries**
- **Business Continuity Firms / Experts**
- **Then, We Synthesize**

October 11 - 13, 1999

Baltimore

- **Overview of HIPAA & Security Drill Down**
- **Reviewed Goals, Objectives, Methodology**
 - **Gathered Issues/ Concerns to Address**
 - **What are you worried about?**
- **Broke Into Tracks**
 - **Business Impact Analysis, Solution Design, Implementations, Monitoring and Reporting**
 - **Led by “Volunteers”**
 - **“Vendor-isms” were discouraged**
- **Report Back Progress**
 - **Ask, Refine, Encourage, Torture, Other**
- **Repeat Steps Above**
- **Close and Go to Next Phase**

3 Breakout Groups

- **Business Impact Analysis**
- **Solution Design and Analysis**
- **Monitoring and Reporting**

- **Approach**
- **Content**

Who Contributed?

| | |
|----------------------------|----|
| Payers | 23 |
| Providers | 39 |
| Consultants | 47 |
| Technology | 22 |
| Clearinghouses | 4 |
| Payer Vendors | 3 |
| Provider Vendors | 10 |
| Government | 10 |
| Professional Organizations | 10 |
| Law Firms | 2 |

Assets We Took Into Summit

- **Highly Refined Raw Material**
 - **By Track**
 - **Refined Matrix**
 - **Toolkit and Tools**
 - **Document Format (Logical Sequence)**
- **Volunteers to Create Finished Product**
- **Web-sites and Communications**
- **A Process**
- **A Timeline**

So, Where Are We Now?

- **Executing the Plan**
 - **Drafting/Revising Guideline Document**
- **Maintaining Focus**
- **Receiving Very Positive Feedback**
- **Reviewers & Validations**
 - **Where you come in**
- **Roll-out Following Final Rules**
- **Looking for Greater Collaboration**
 - **CPRI-HOST**

Going Forward

- **Coordinate and Proliferate (with Your Help)**
- **Refine and Improve**
 - Your / Our Guidance (Leverage Experience)
- **Additional Thoughts? Send w/ Subject to:**
 - hipaa.issues@smed.com
- **Remain Coordinated w/ NPRM Timing**
- **Stay Tuned for Updates and Deliverables at**

www.smed.com/hipaa

www.wedi.org

Thank you!