

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 *HIPAA Privacy & Security Assistant*
- CPRI-HOST *Confidentiality and Security Training Video*
- NCHICA's *HIPAA EarlyViewÔ*
- SEI's *Self Risk Assessment Tool*
- WEDI's *HIPAA Security Summit Implementation Guidelines*
- AAMC *Guidelines for Academic Medical Centers on Security and Privacy*

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

The screenshot shows a Microsoft Internet Explorer browser window with the title bar "CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente". The address bar contains the URL "http://www.cpri-host.org/toolkit/toc.html". The page content includes the CPRI-HOST logo with the tagline "Advancing Electronic Information Systems for Health Care" and the CPRI Toolkit logo with the tagline "Computer-based Patient Record Institute". A navigation menu lists: Home, About Us, Membership, Meetings, Davies Award, Members Only, Resources, Committees, Task Forces, and Contact Us. The main heading is "CPRI Toolkit: Managing Information Security in Health Care, Version 3" in red, with navigation links: < back | table of contents | content committee | next >. Below this is a box titled "CPRI Toolkit Table of Contents" containing two items: a PDF icon followed by "Download Entire Toolkit in Adobe Acrobat - PDF Format (1.58 MB)" and another PDF icon followed by "1.0 Executive Summary". The status bar at the bottom shows "Done" and "Internet".

CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address <http://www.cpri-host.org/toolkit/toc.html> Go

CPRI-HOST
Advancing Electronic Information Systems for Health Care

CPRI Toolkit
Computer-based Patient Record Institute

Home About Us Membership Meetings Davies Award Members Only Resources Committees Task Forces Contact Us

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

< back | table of contents | content committee | next >

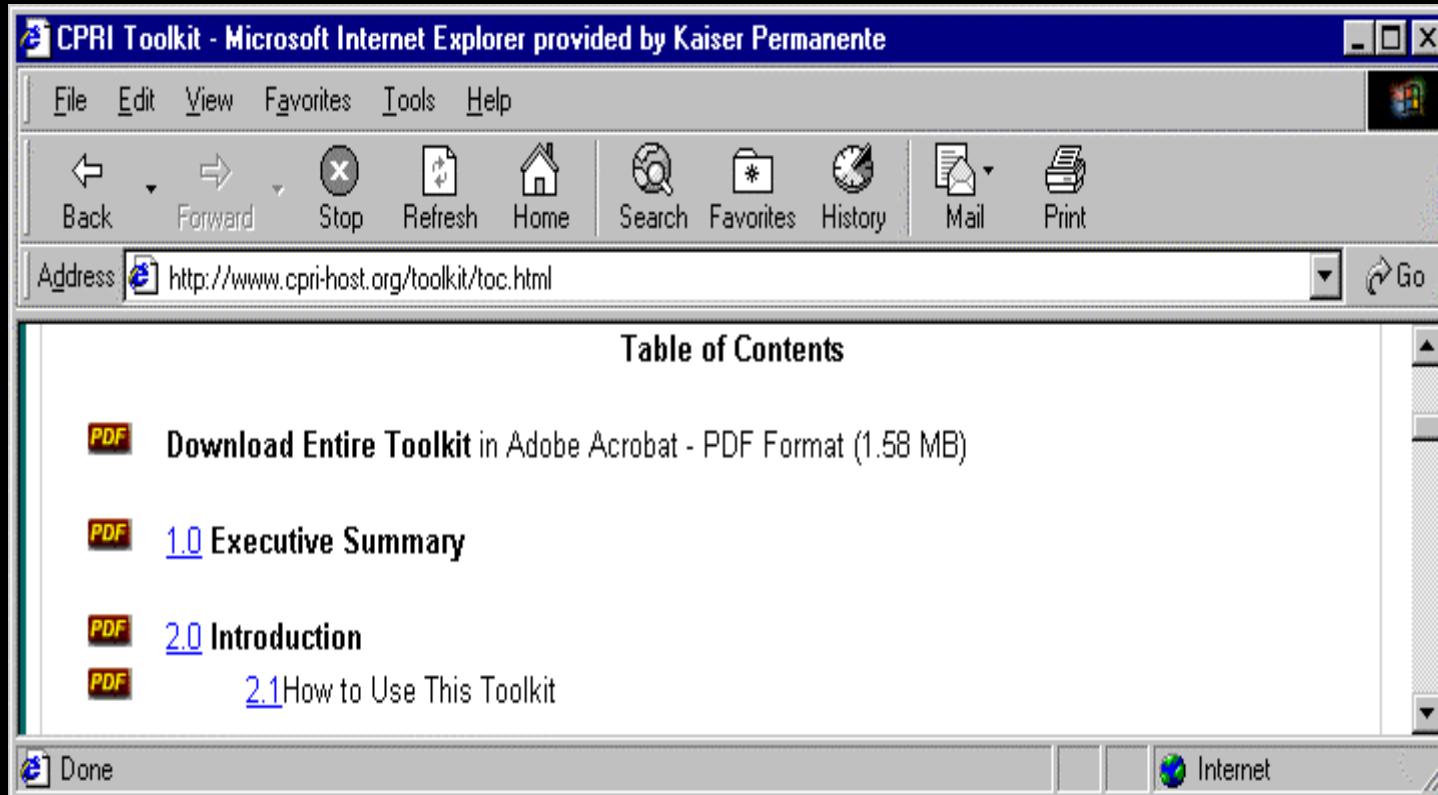
CPRI Toolkit
Table of Contents

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

PDF [1.0 Executive Summary](#)

Done Internet

Toolkit - Sections 1 & 2



Toolkit - Section 3


















CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

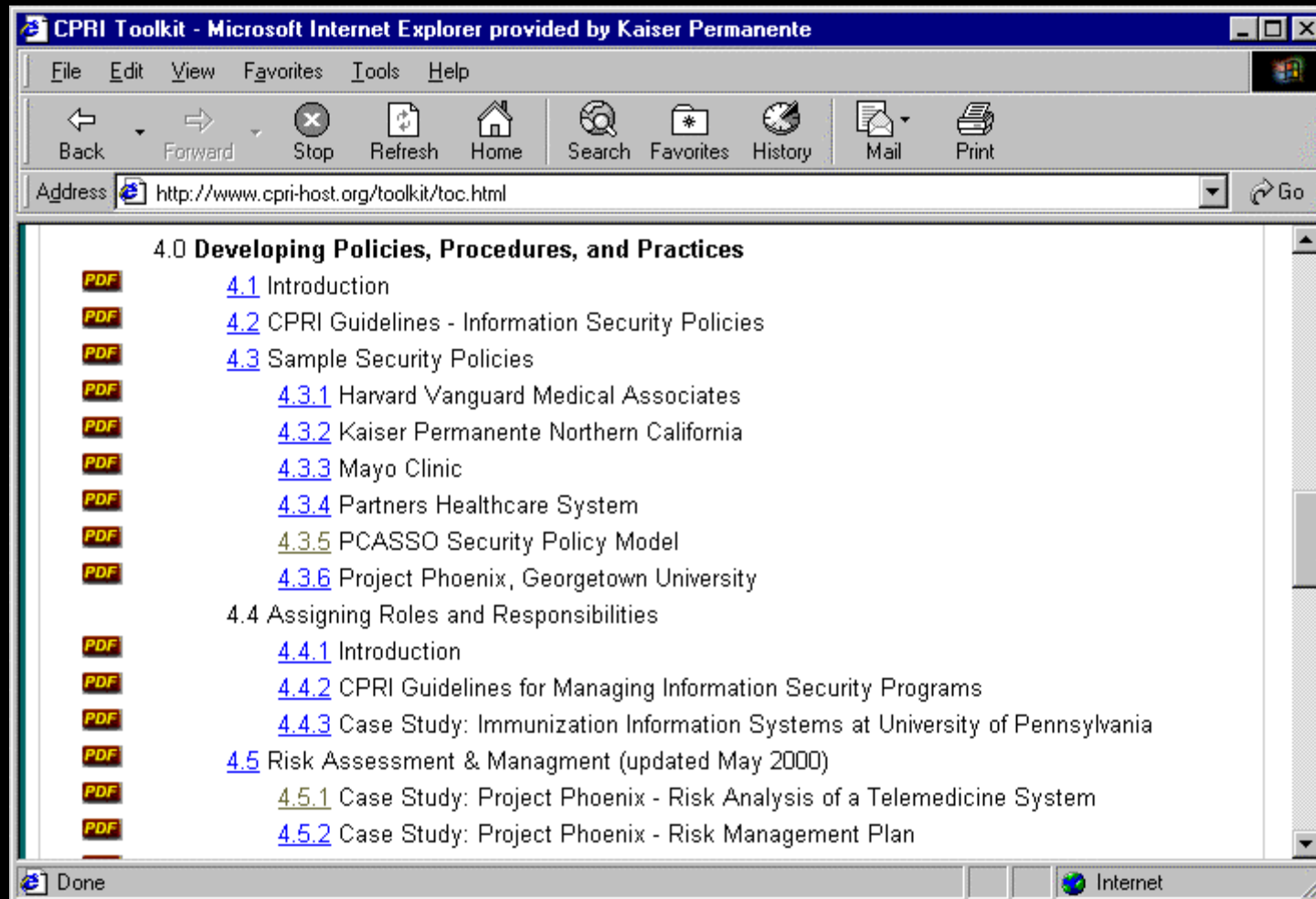
Address <http://www.cpri-host.org/toolkit/toc.html> Go

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](#)
-  [3.8 EU Privacy Directive \(updated May 2000\)](#)

Done Internet

Toolkit - Section 4.0 - 4.5.2



The screenshot shows a Microsoft Internet Explorer browser window titled "CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente". The address bar displays "http://www.cpri-host.org/toolkit/toc.html". The main content area lists the following items:

- 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](#)
 - [4.4.2 CPRI Guidelines for Managing Information Security Programs](#)
 - [4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania](#)
 - [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](#)

The status bar at the bottom shows "Done" and "Internet".

Toolkit - Section 4.6 - 4.10

CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

File Edit View Favorites Tools Help

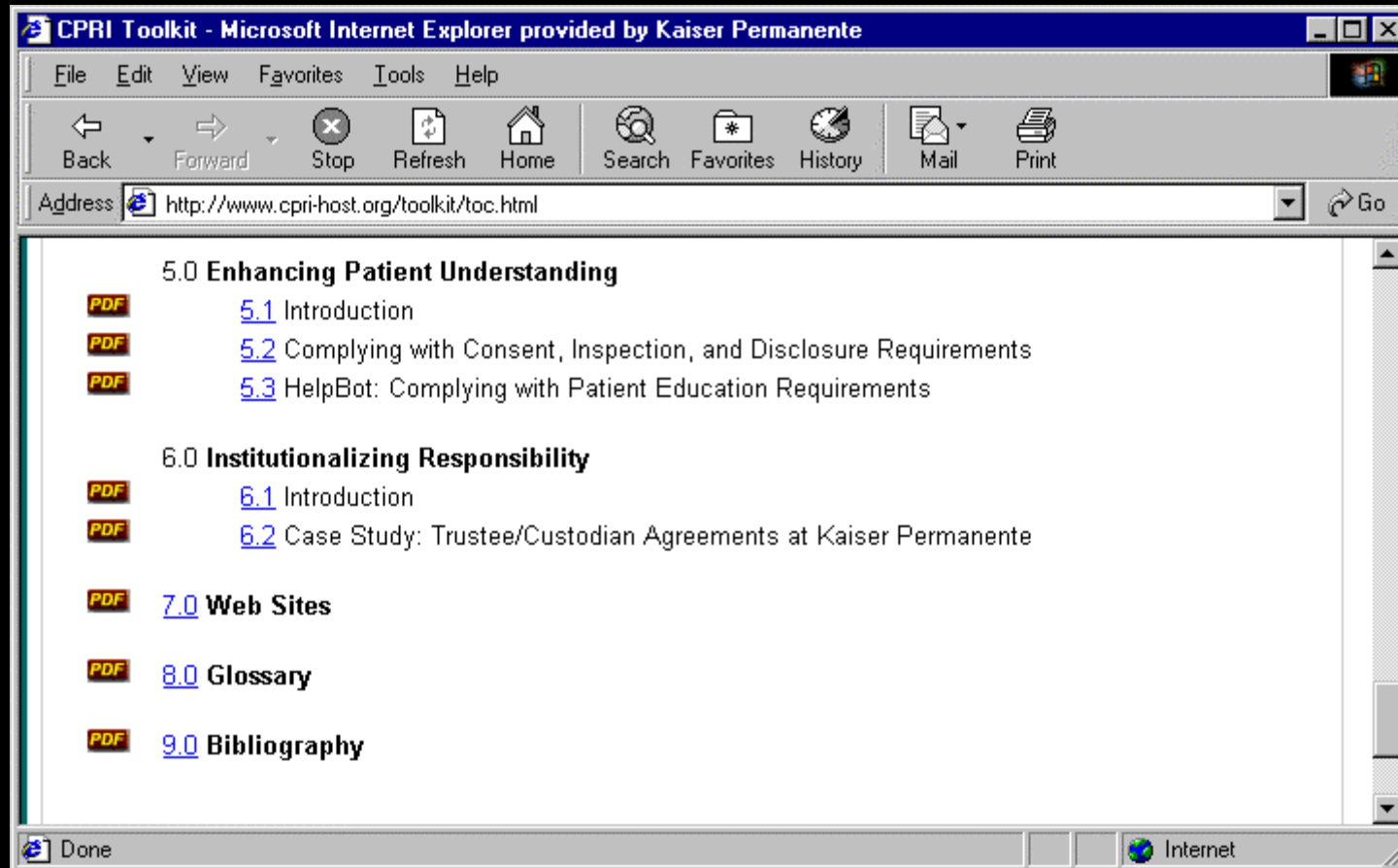
Back Forward Stop Refresh Home Search Favorites History Mail Print

Address <http://www.cpri-host.org/toolkit/toc.html> Go

	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)

Done Internet

Toolkit - Section 5-9



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 - “Safeharbor”

Toolkit - Section 3

CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

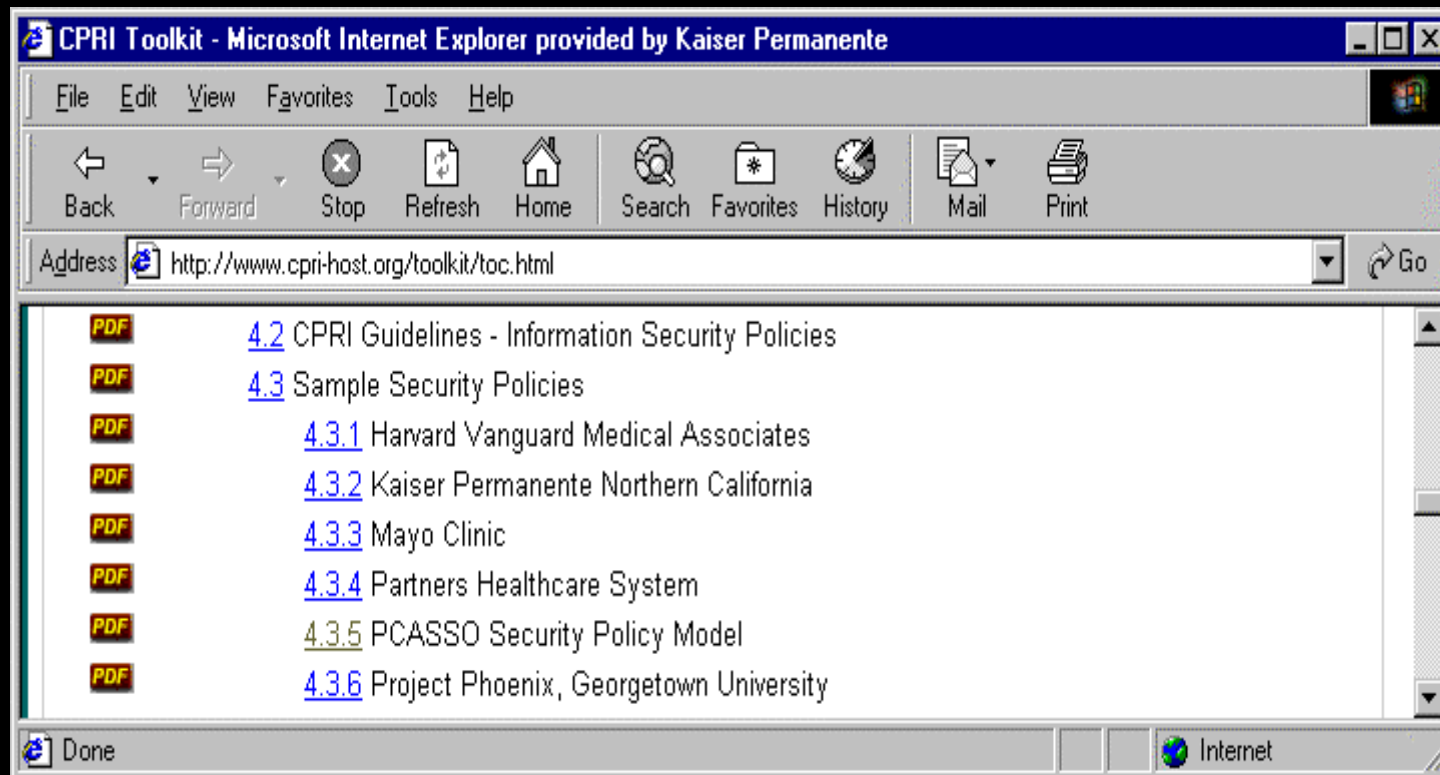
Address <http://www.cpri-host.org/toolkit/toc.html> Go

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](#)
- [3.8 EU Privacy Directive \(updated May 2000\)](#)

Done Internet

Information Security Policies

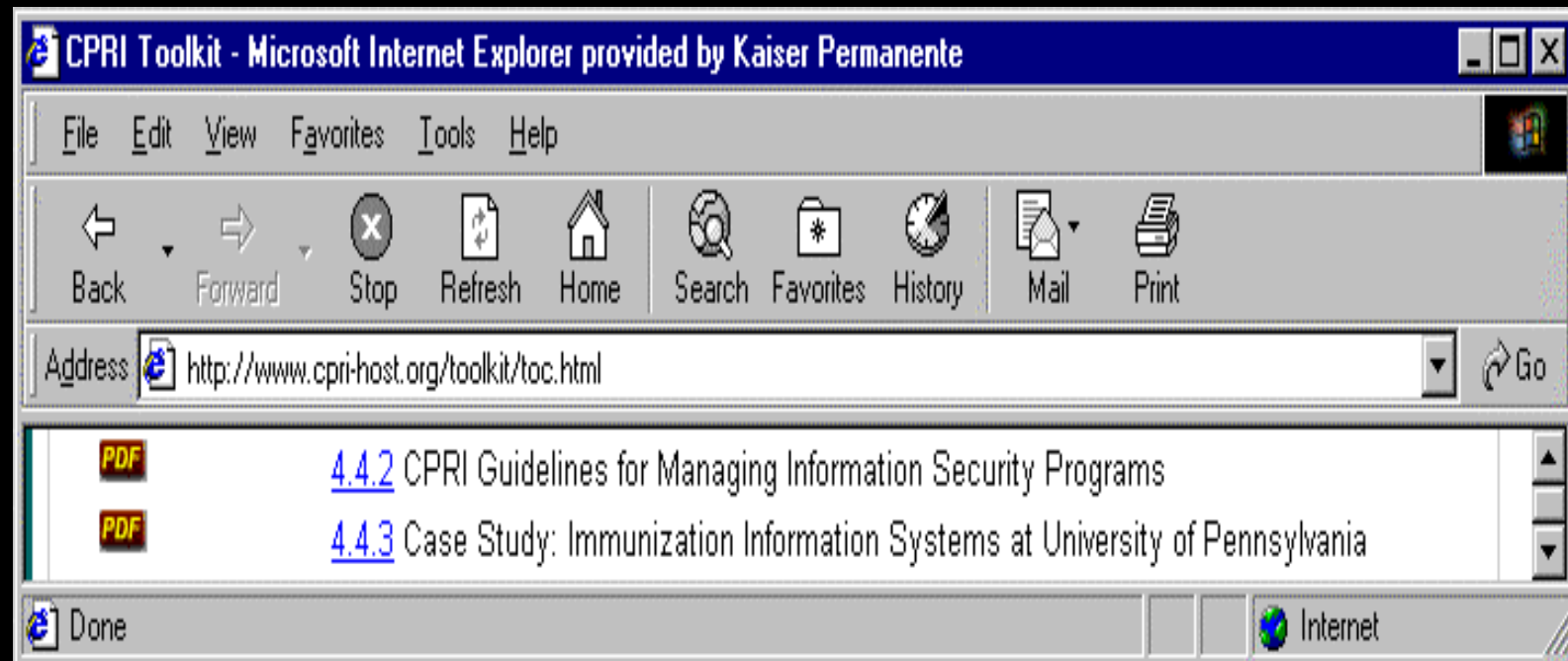


Toolkit & Critical Steps

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

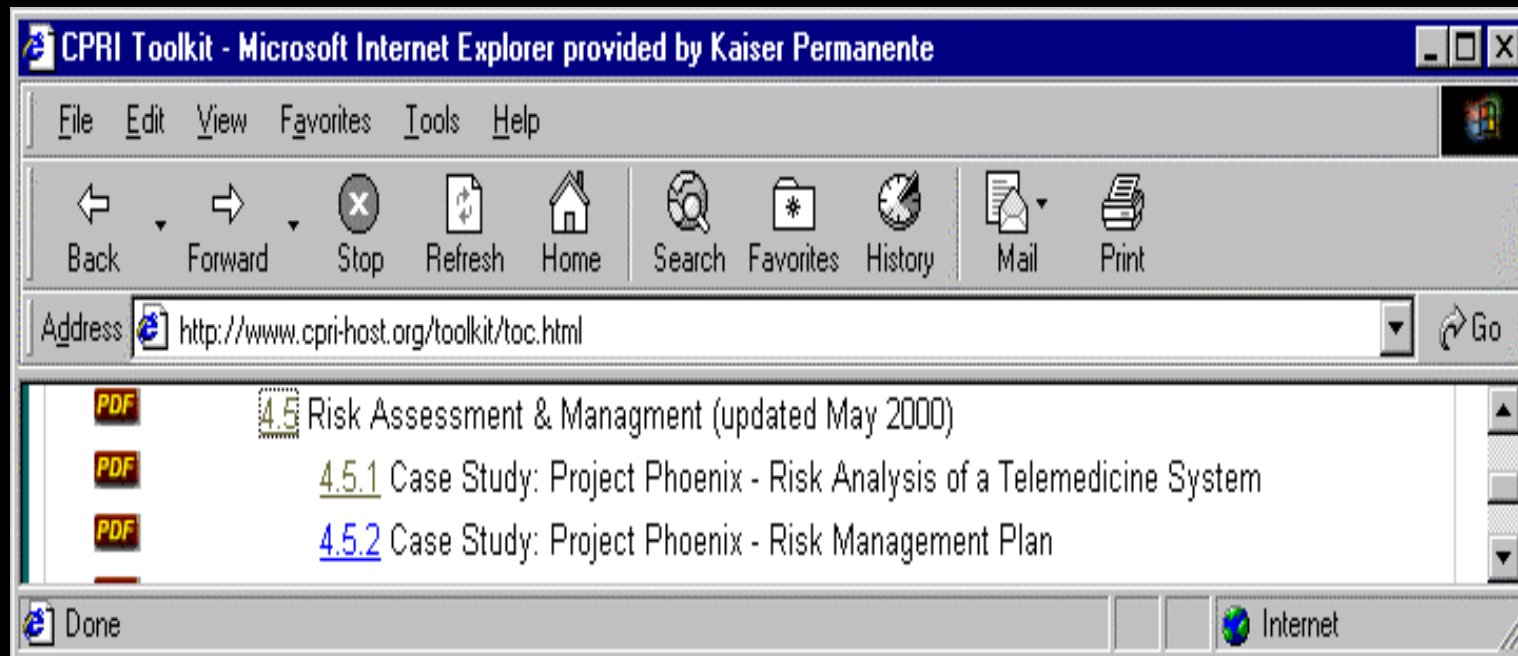


Toolkit & Critical Steps

3. Building Risk Management Capability

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

Building Risk Management Capability

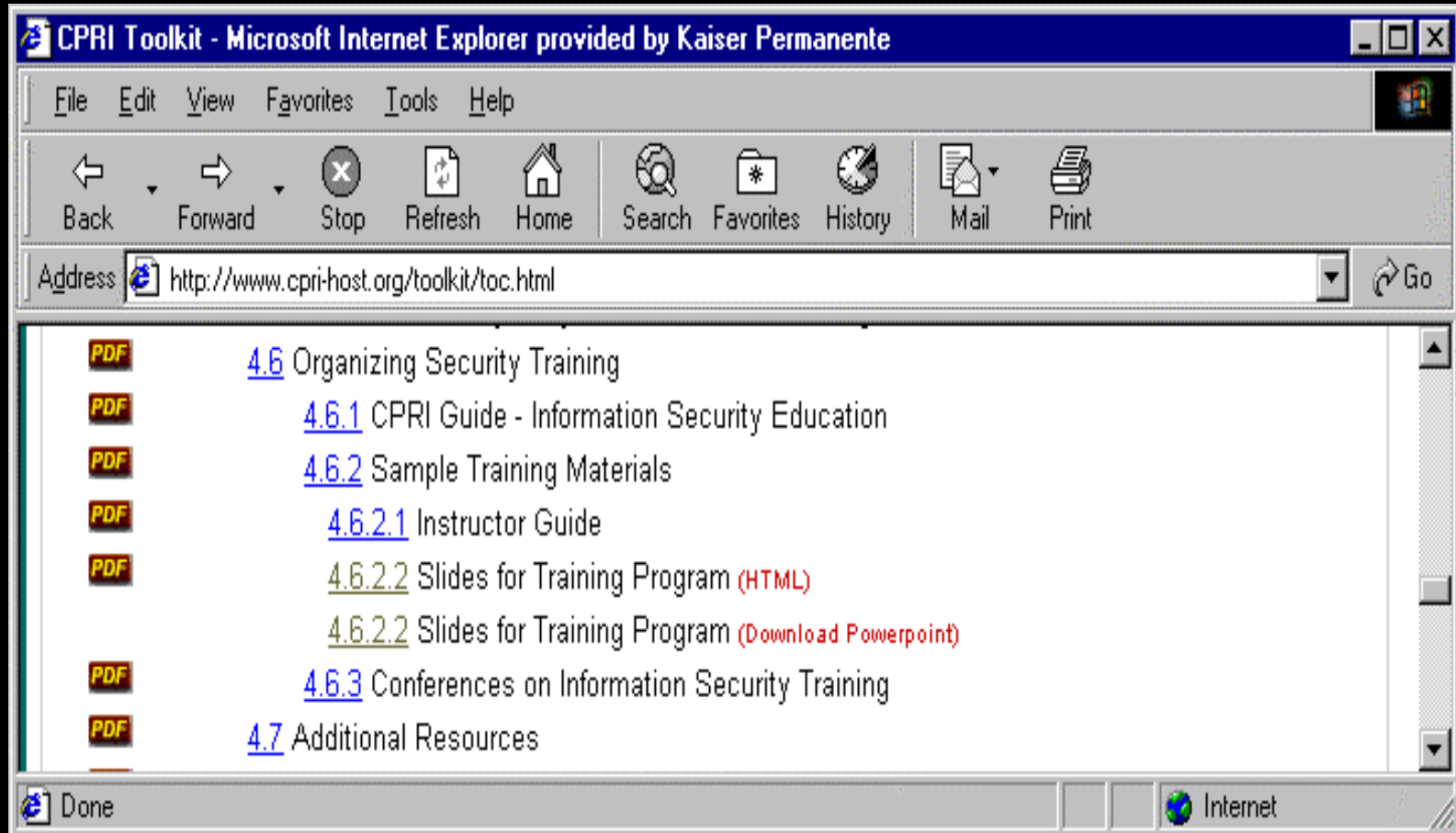


Toolkit & Critical Steps

4. Driving enterprise-wide awareness

- *Information Security Education - 4.6*
 - CPRI Guide on security training - 4.6.1
 - Sample Instructor's guide and slides - 4.6.2

Information Security Education

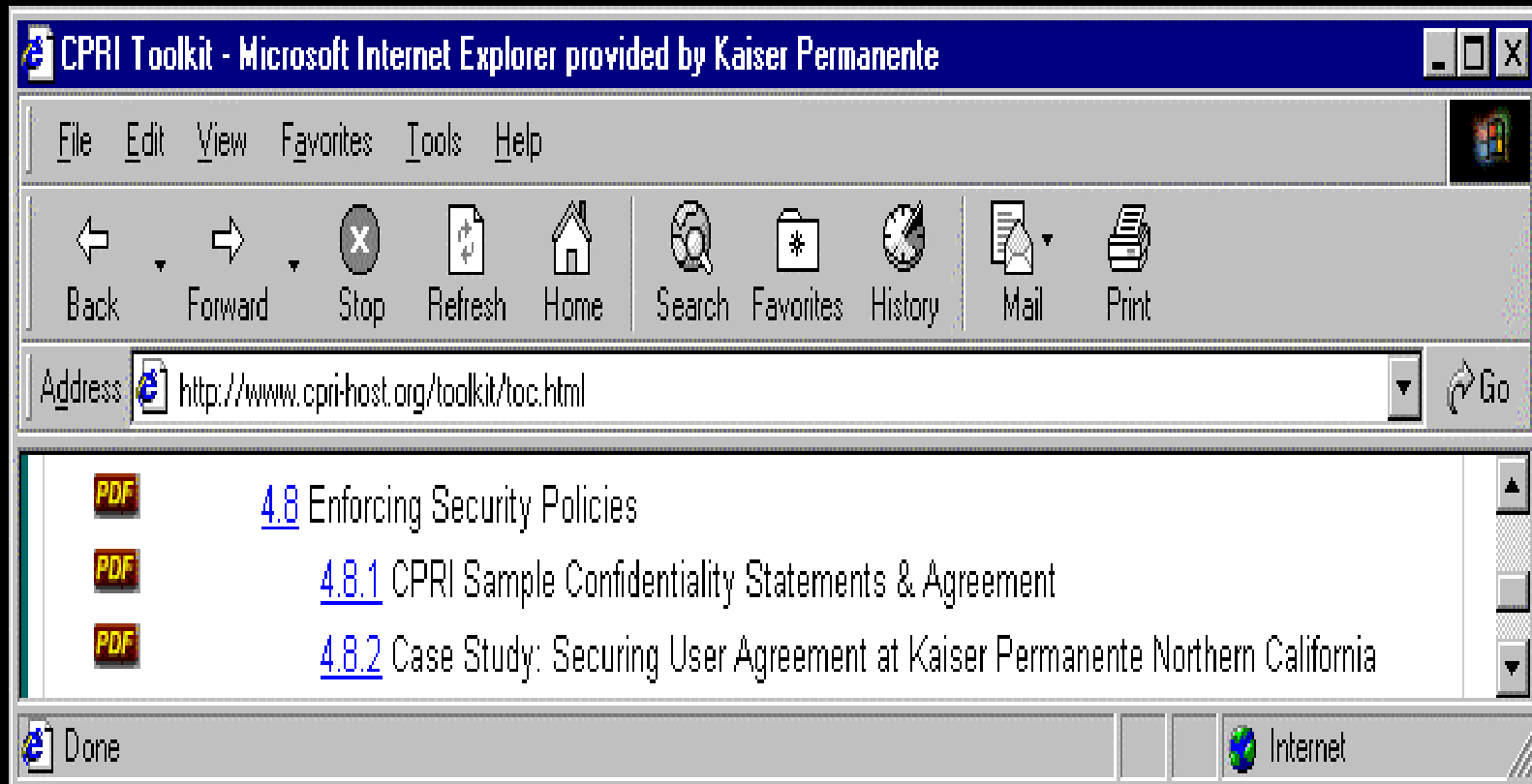


Toolkit & Critical Steps

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

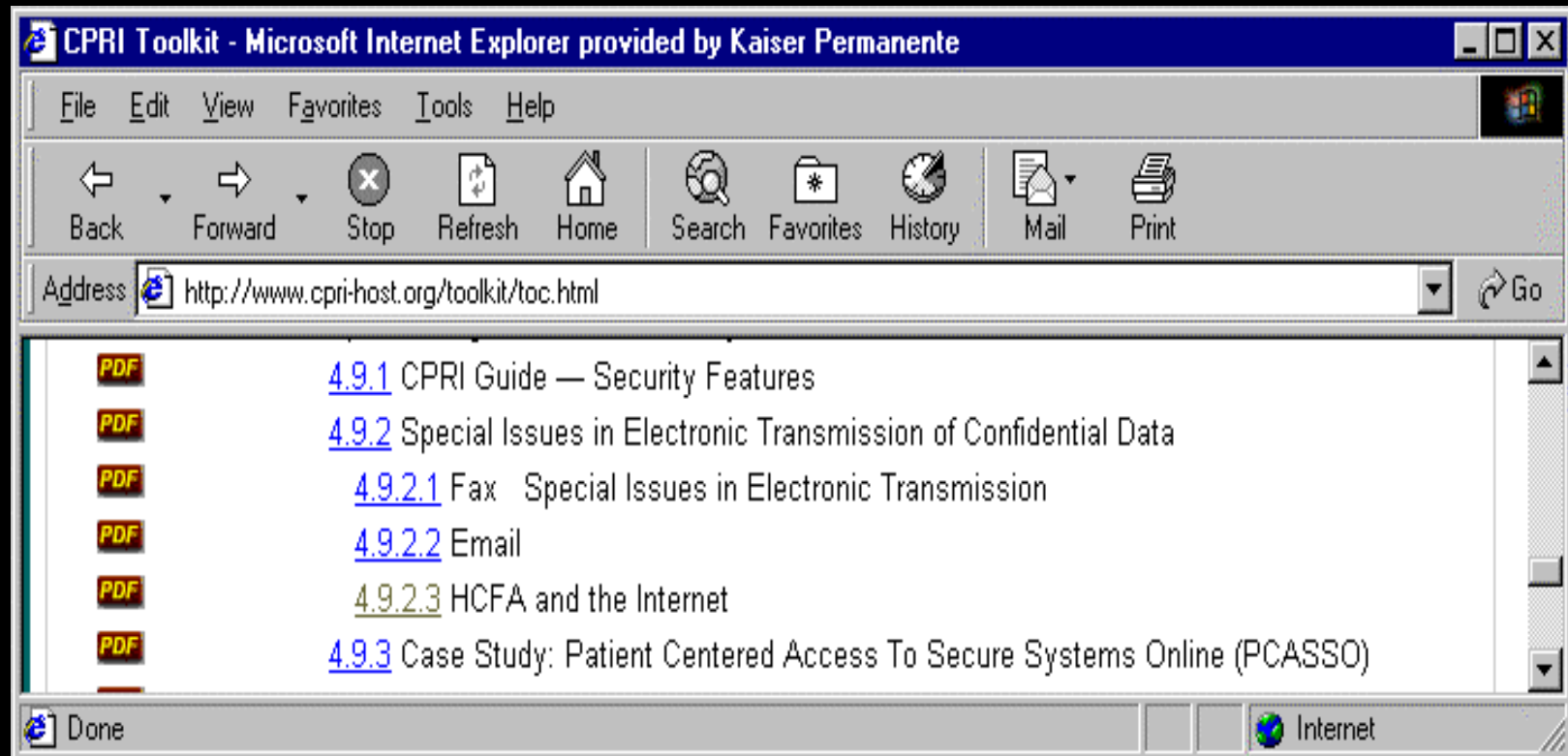


Toolkit & Critical Steps

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

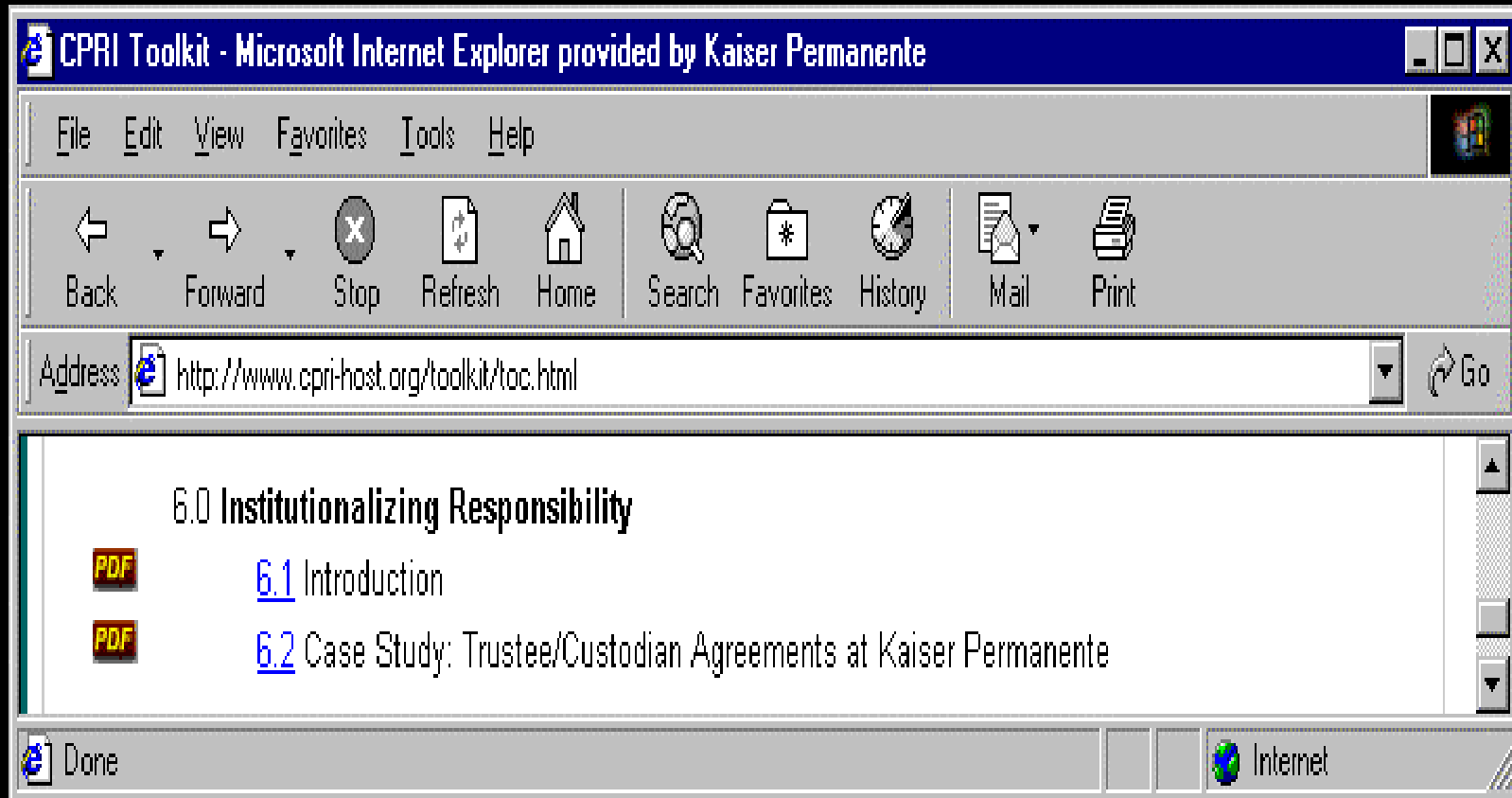


Toolkit & Critical Steps

7. Institutionalizing Responsibility

- Kaiser's Trustee-Custodian Agreement

Institutionalizing Responsibility

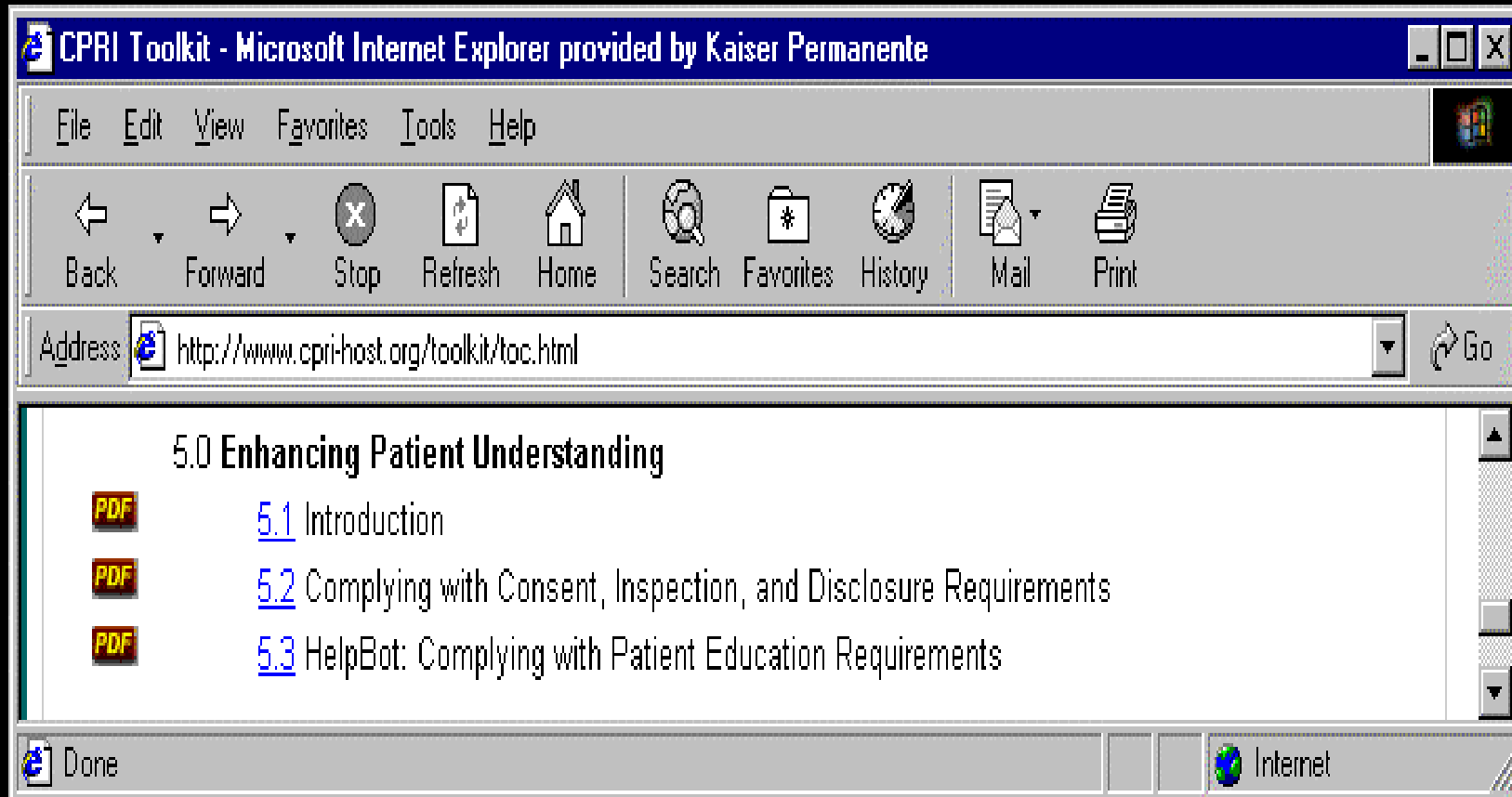


Toolkit & Critical Steps

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



Results

**Enhanced judgement
in managing health information**

**Improved health care information
security**

CPRI-HOST HIPAA

Privacy & Security Assistant

- Microsoft Access Database Application
- Displays each HIPAA
 - Requirement/Section
 - Implementation Feature
 - “HIPAA in Plain English”
- Provides for your entry of
 - Items needed to be done to address each
 - A description of each item you enter
 - Task assignment and tracking

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



Disclaimer

The CPRI-HOST HIPAA Privacy and Security Assistant should only be used as an help understand the regulations and to identify and define what needs to be done by your organization to become compliant with the HIPAA privacy and security regulations .

The content provided in this database should not be adopted by any organization without review by the individual responsible for privacy and security, the organization's legal council and those with authority to set policy.

CPRI-HOST accepts no responsibility for losses incurred through the use the CPRI-HOST HIPAA Privacy and Security Assistant.

[Click here for an explanation of the HIPAA privacy and security regulations in plain English.](#)

[Click here to identify and define what needs to be done to address the HIPAA privacy and security regulations.](#)



Privacy Regulations in Plain English | Security Regulations in Plain English

HIPAA #

160

HIPAA
Privacy
Text



For the reasons set forth in the preamble, 45 CFR Subtitle A, Subchapter C, is amended as follows:

1. Part 160 is revised to read as follows:

PART 160 GENERAL ADMINISTRATIVE REQUIREMENTS

Subpart A General Provisions

160.101 Statutory basis and purpose.

160.102 Applicability.

160.103 Definitions.

160.104 Modifications.

Subpart B Preemption of State Law

160.201 Applicability

160.202 Definitions.

160.203 General rule and exceptions.

160.204 Process for requesting exception determinations.

160.205 Duration of effectiveness of exception determinations.

Subpart C Compliance and Enforcement

160.300 Applicability.

HIPAA in
Plain
English

This section is a list of the parts and subparts of the HIPAA privacy regulation.

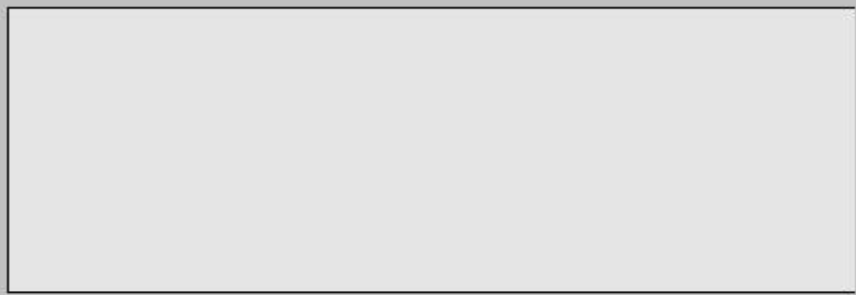


Privacy Regulations in Plain English Security Regulations in Plain English

HIPAA Category	Administrative Procedure	HIPAA Number	142.308.a.1
Requirement	Certification	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.



Plain English Explanation

Certification
The regulation requires organizations to certify security controls. An internal organization or a third party can do certification, and no specific certification process or regime is identified by regulation.

The purpose of certification is to assess and document that the items included in the organization's security plan have been implemented and are in effect for each of the organization's computer system and networks. The "pre-specified set of security requirements" is the list of items that were placed in the security plan as the result of business decisions resulting from preceding documented and formal HIPAA required processes of risk assessment, management and mitigation.

Covered entities will have to "certify" that their efforts to mitigate data security risks have implemented the standards established during their own risk assessment. This requirement emphasizes the "life-cycle" approach to risk management outlined as part of the security management process regulation and thereby brings risk management full circle. Good risk management plans become incorporated into everyday practice and do not disappear into an administrative drawer once signed. By documenting that they are providing the level of protection promised at the beginning of the process, covered entities demonstrate their compliance with this fundamental strategic goal of health information assurance.



The Computer-based Patient Record Institute - Healthcare Open Systems and Trials (CPRI-HOST)HIPAA Privacy and Security Assistant is a software tool made available to help organizations understand the HIPAA privacy and security regulations and to identify what they will need to do to address them.

It is designed to help an organization use a systematic process to identify and track the individual items needed for each of the HIPAA privacy and security regulations.

The Assistant takes a slightly different approach to the privacy regulations than it does to the security regulations. For the HIPAA privacy regulations it displays each section of the regulations and for the security regulations, each requirement and implementation feature is individually displayed. For both data entry tables are provided to capture the items that need to be addressed. Different approaches were taken because of the different structures of the privacy and security regulations.

This tool also has functions for managing the items identified to be addressed. A number of reports are available and the data may be output to a word-processing or spreadsheet file. It is possible to import these files into project management software.

The tabs above, display the different areas of functionality. The reference section provides direct links to Internet resources.

The CPRI-HOST HIPAA Privacy and Security Assistant was developed by Ted Cooper, MD.

[HIPAA in Plain English](#)



HIPAA Category Security Standard Introduction
 Requirement Security Standard Introduction

HIPAA Number 142.308
 Implementation Feature Approach to HIPAA Introduction

§ 142.308 Security standard.
 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:

Each affected entity 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.
 The standard does not address the extent to which a particular entity should implement the specific features. Instead, we would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.

[HIPAA in Plain English](#)

For each requirement or 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
Risk Assessment	We will have a formal risk assessment project.
Risk Management Plan	After we assess our risks we will determine the policies, procedures and technology that we will implement to address the risks for which the costs of doing so are less than the value of what we would likely lose by not doing so.
Assign Authority for Decision Making	We will need a process or individual to make the decisions involved in the risk management plan.
HIPAA in Plain English	A formal risk assessment and risk management plan will need to be documented. Each requirement will need to be addressed, but the specific measures and the extent of the measures employed to address each requirement is a business decision for the organization. HIPAA does not spell out the details of what and how each requirement must be addressed.
*	



HIPAA Category Security Standard Introduction

HIPAA Number 142.308

Requirement Security Standard Introduction

Implementation Feature Approach to HIPAA Introduction

§ 142.308 Security standard.
 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:

Each affected entity 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.
 The standard does not address the extent to which a particular entity should implement the specific features. Instead, we would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements. How individual security requirements would be satisfied and which technology to use would be business decisions that each organization would have to make.

[HIPAA in Plain English](#)

Assign Tasks

HIPAA Number	142.308	Description of What Needs to Be Done	We will have a formal risk assessment project.
Concept	Risk Assessment		
Assigned To	Sharon	Comment	This is the key to future success.
Date Due	02/20/2001		
Status	unreviewed		
Next Status	01/31/2001		

Record: 1 of 4

- Report "Assigned To"
- Report "Date Due"
- Report "Next Status Check"
- Report "Status"
- Send Report to a File



Search

§ 142.103 Definitions.

For purposes of this subpart, the following definitions apply:

Code set

means any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes.

Health care clearinghouse

means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements. The entity receives health care transactions from health care providers or other entities, translates the data from a given format into one acceptable to the intended payer or payers, and forwards the processed transaction to appropriate payers and clearinghouses. Billing services, repricing companies, community health management information systems, community health information systems, and "value-added" networks and switches are considered to be health care clearinghouses for purposes of this part.

Health care provider

means a provider of services as defined in section 1861(u) of the Social Security Act, 42 U.S.C. 1395x, a provider of medical or other health services as defined in section 1861(s) of the Social Security Act, and any other person who furnishes or bills and is paid for health care services or supplies in the normal course of business.

Health information

means any information, whether oral or recorded in any form or medium, that (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health plan

means an individual or group plan that provides, or pays the cost of, medical care. Health plan includes the following, singly or in combination:

(1) Group health plan. A group health plan is an employee welfare benefit plan (as currently defined in section 3(1) of the Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, or otherwise, and

(i) Has 50 or more participants; or

(ii) Is administered by an entity other than the employer that established and maintains the plan.

(2) Health insurance issuer. A health insurance issuer is an insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.



References

Title	URL	Description
▶ 11-19 Working Group	www.11-19.org	The 11-19 Working Group comprises healthcare companies and organizations with a common interest: the desire to advance the best and most proven security standards for Internet healthcare systems and transactions.
Administrative Simplification	http://aspe.os.dhhs.gov/dmnsimp/	In formation on HIPAA administration simplification at the Department of Health and Human Services.
AMA/CEJA	www.ama-assn.org	Numerous guidelines and resources, e.g.: AMA Web Guidelines; CEJA E-10.01 Fundamental Elements of Patient - Physician Relationship; CEJA E-5.07 Confidentiality: Computers
American Academy of Pediatrics	www.aap.org	Privacy Protection of Health Information: Patient Rights and Pediatrician Responsibility (Pediatrics, Volume 104, Number 4, 973-977)
American Health Information and Management Association (AHIMA)	http://www.ahima.org	The AHIMA web site has a number of products and publications that support HIPAA privacy and security standards.
American Health Lawyers Association	www.healthlawyers.org	

Record: 1 of 82

Preview Reference List

Print Reference List

CPRI-HOST Confidentiality and Security Training Video

- *What if it were yours?*
- Donated to CPRI-HOST by Kaiser Permanente
- www.cpri-host.org



HIPAA Proposed Security Regulation Self-evaluation Tool

NCHICA

Uses of *HIPAA EarlyView*®

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

Greeting



NCHICA

HIPAA EarlyViewTM

Version 1.0

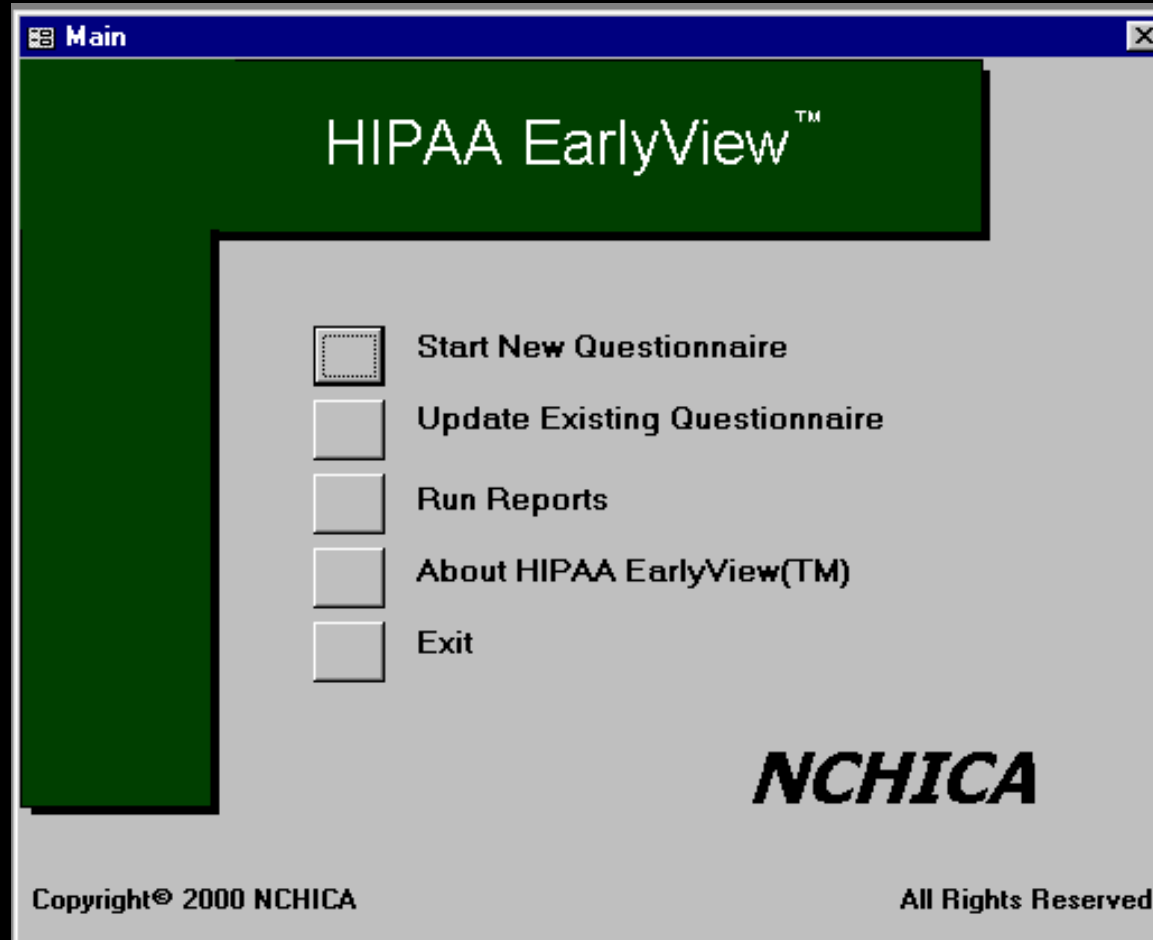
HIPAA Security Proposed Regulation Self-Evaluation Tool

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



Copyright 2000 NCHICA All Rights Reserved

Main Menu



Enter Contact Data

Contact Information Form

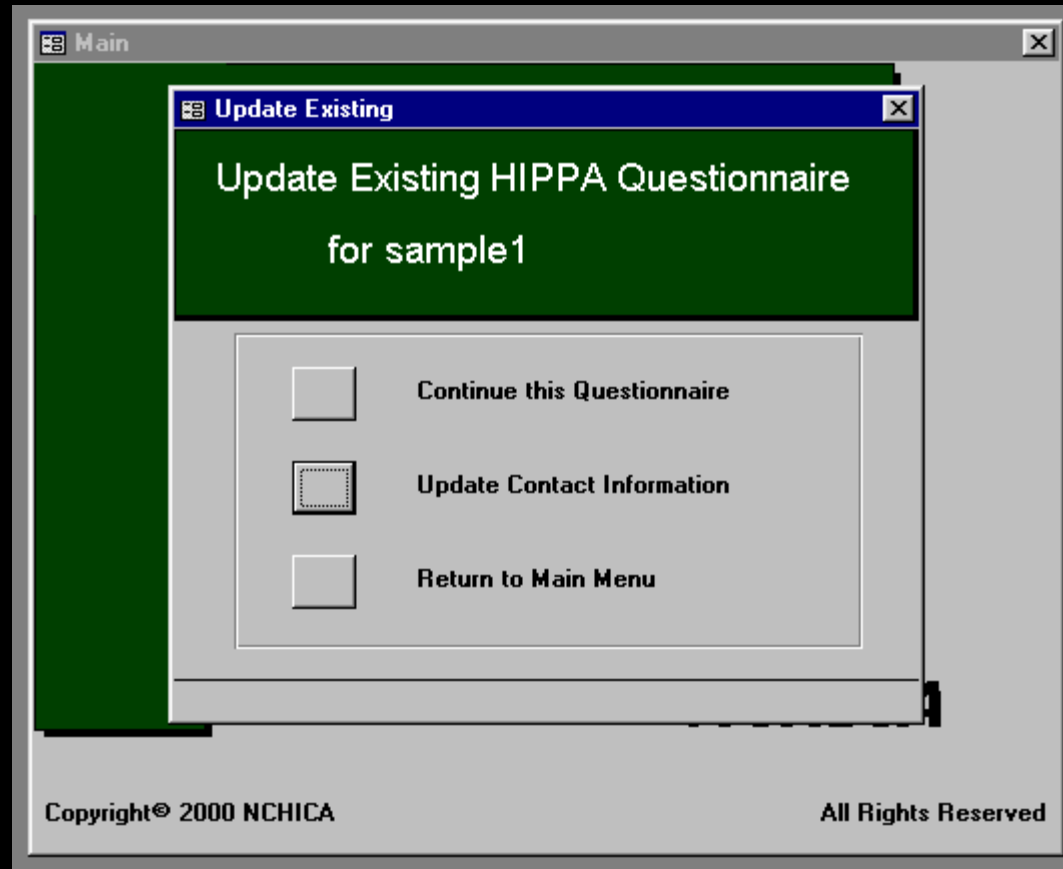
HIPAA Security Questionnaire Contact Data

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/Y		
Address1	<input type="text" value="Addr1"/>	Due Date	<input type="text" value="12/31/00"/> M/D/Y		
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."/>		
	Zip	<input type="text" value="99999-9999"/>	F. E-Mail	<input type="text" value="facilitator@sampel.com"/>	
Phone	<input type="text" value="(999) 999-9999 Ext."/>	Fax	<input type="text" value="(999) 999-9999"/>	Serial #	<input type="text" value="1234"/>
E-Mail	<input type="text" value="email@sample.com"/>				

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

Update Questionnaire Menu

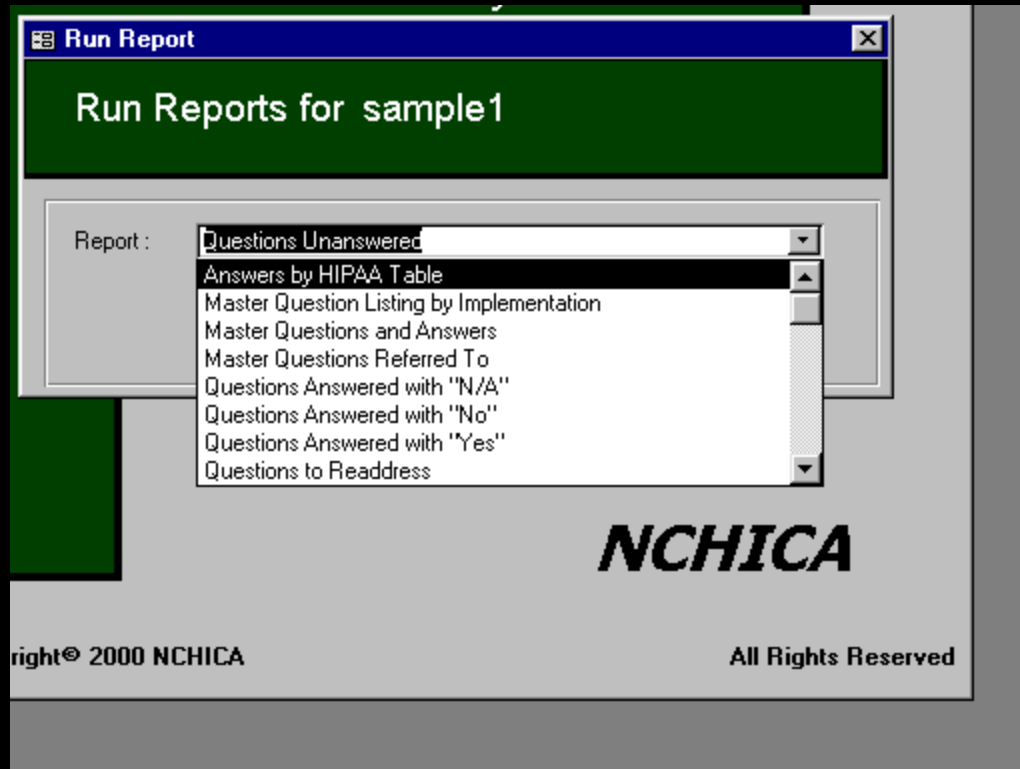


Security Questions

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:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A <input type="radio"/> Unanswered	Due Diligence Demonstrated: <input type="checkbox"/> 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: <input type="checkbox"/>

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)



Carnegie Mellon
Software Engineering Institute

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)



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

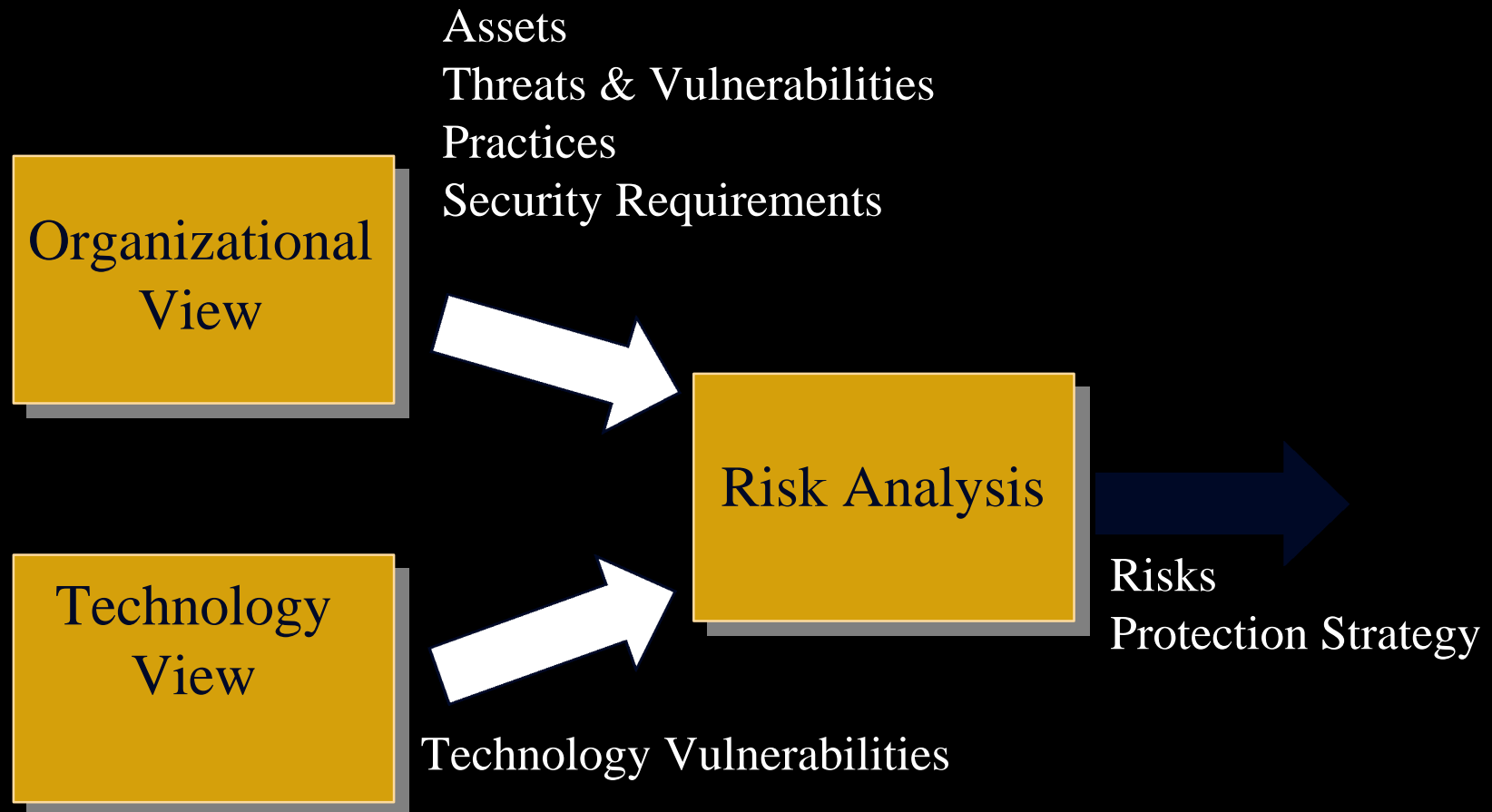


Benefits

- 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



HIPAA Security Summit Implementation Guidelines

- Lead by Roger May
- Sponsors - IBM, TRW, COMPAQ, KSM Healthcare Resources, Johns Hopkins, Microsoft, SMS
- WEDI - infrastructure support

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???

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

Going Forward

- Now a part of WEDI/SNIP

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

- View Current Draft at

<http://www.wedi.org/public/articles/details.cfm?id=42>

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*

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

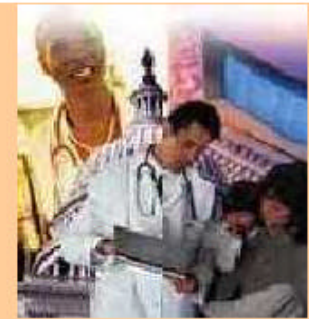
- **CPRI-HOST**
- **Health Care Financing Administration**
- **Healthcare Computing Strategies, Inc.**
- **North Carolina Healthcare Information and Communications Association**
- **Southeastern University Research Association**
- **Workgroup on Electronic Data Interchange**

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: [Consent 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 Guideline](#)

[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](#), [Internet 2](#), [Object Management Group](#), and [Workgroup on Electronic Data Interchange](#). The workshop participants analyzed current health information security and privacy polices, 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.

AAMC Guidelines

- Is available on web sites
 - AAMC
 - WEDI
 - www.amc-hipaa.org

Thank you!