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 asses 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 EarlyViewÔ*
- 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!

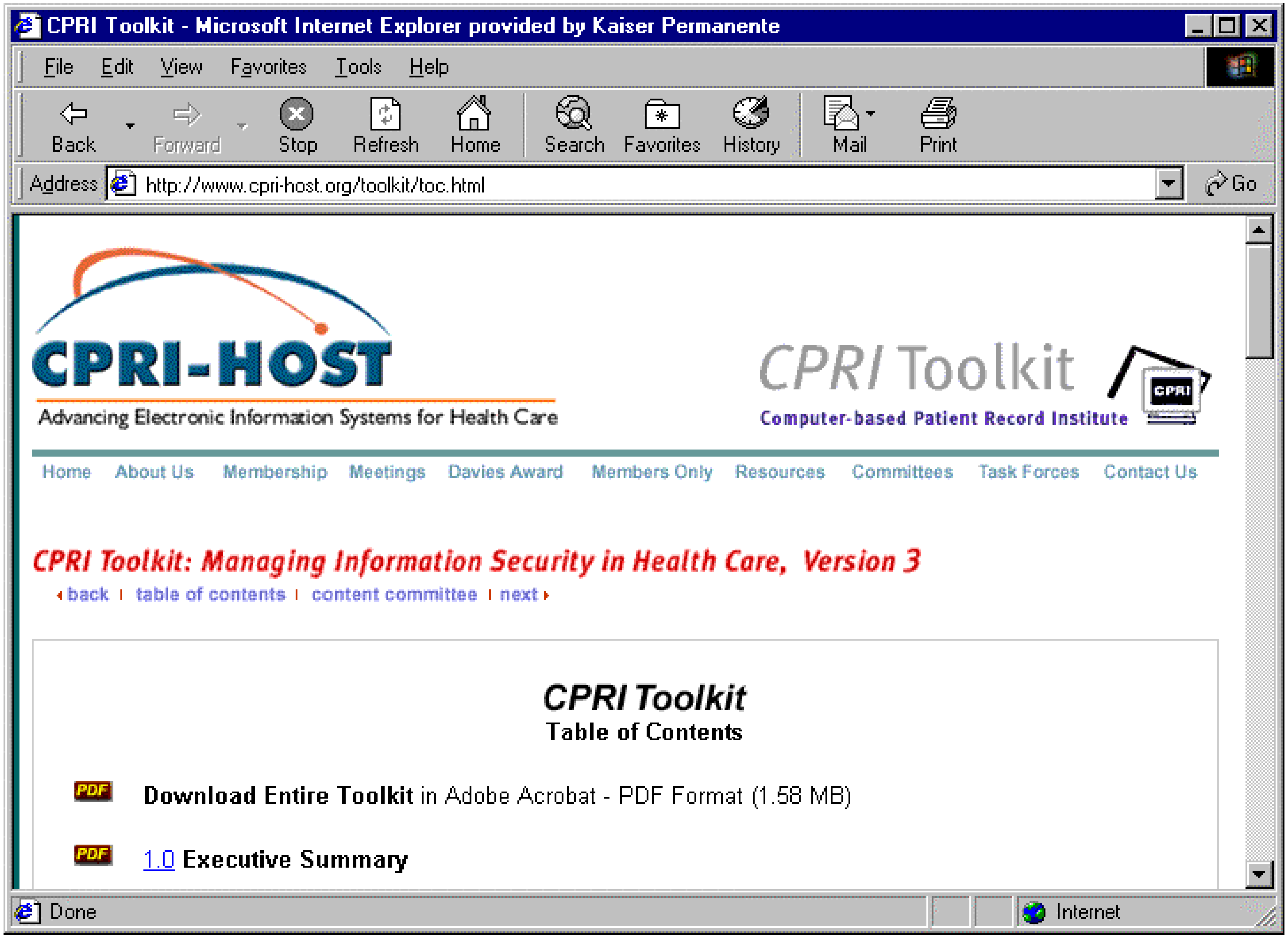
Security Program Functions

- 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 - 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
back | table of contents | content committee | next
Done
Internet

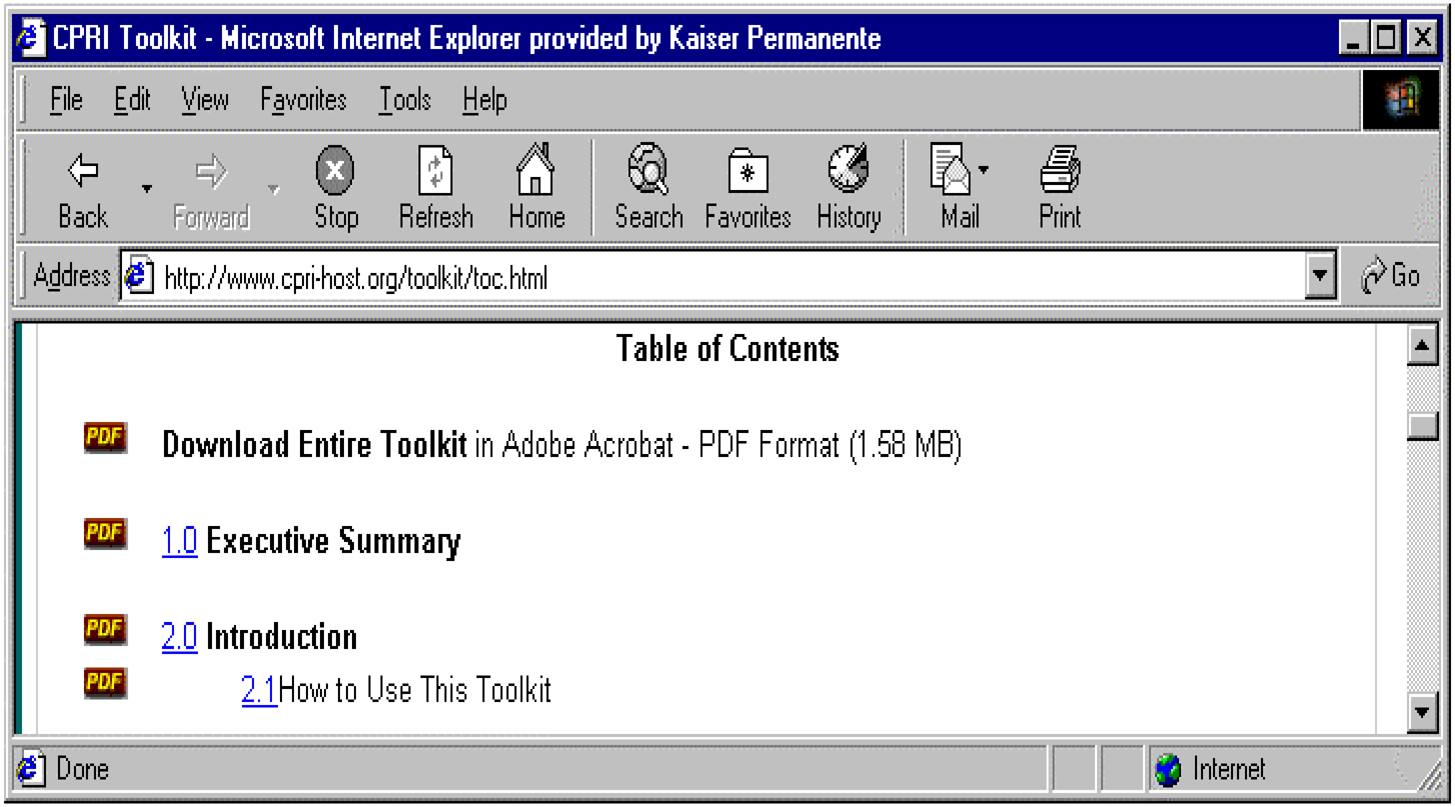
CPRI Toolkit: Managing Information Security in Health Care, Version 3

CPRI Toolkit
Table of Contents

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

PDF 1.0 **Executive Summary**

Toolkit - Sections 1 & 2



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
Done
Internet

Table of Contents

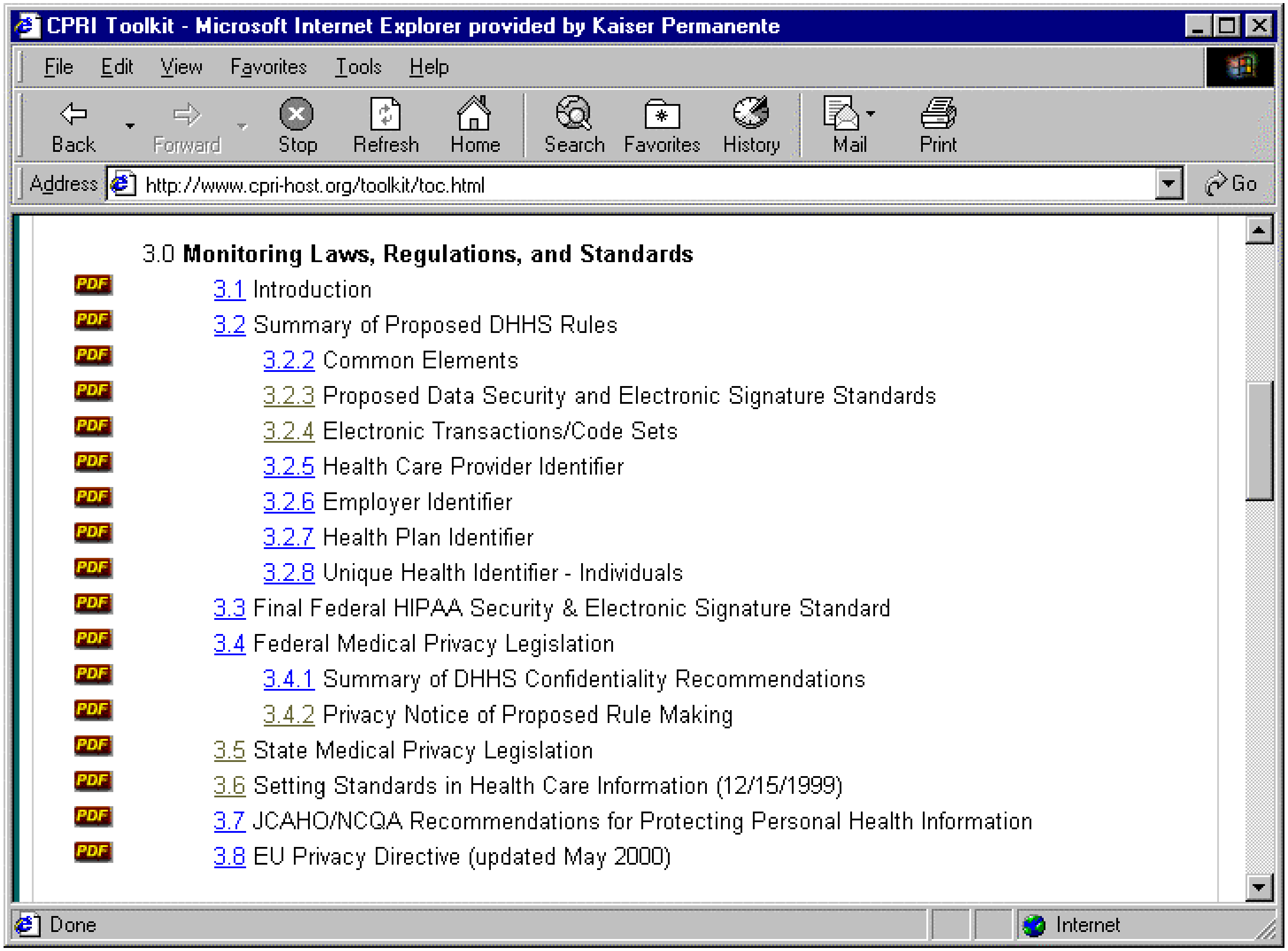
PDF **Download Entire Toolkit** in Adobe Acrobat - PDF Format (1.58 MB)

PDF 1.0 **Executive Summary**

PDF 2.0 **Introduction**

PDF 2.1How to Use This Toolkit

Toolkit - Section 3

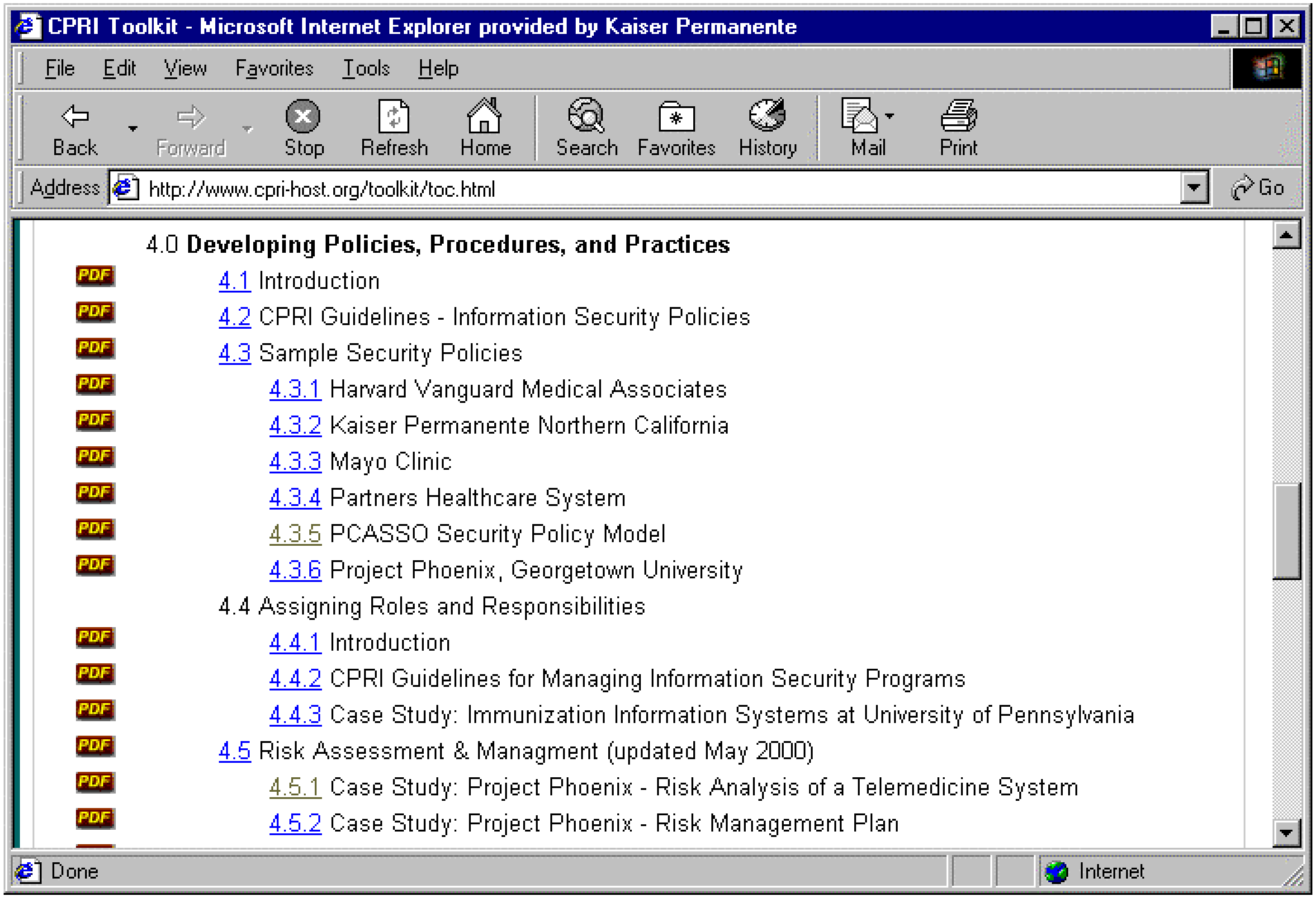


CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

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

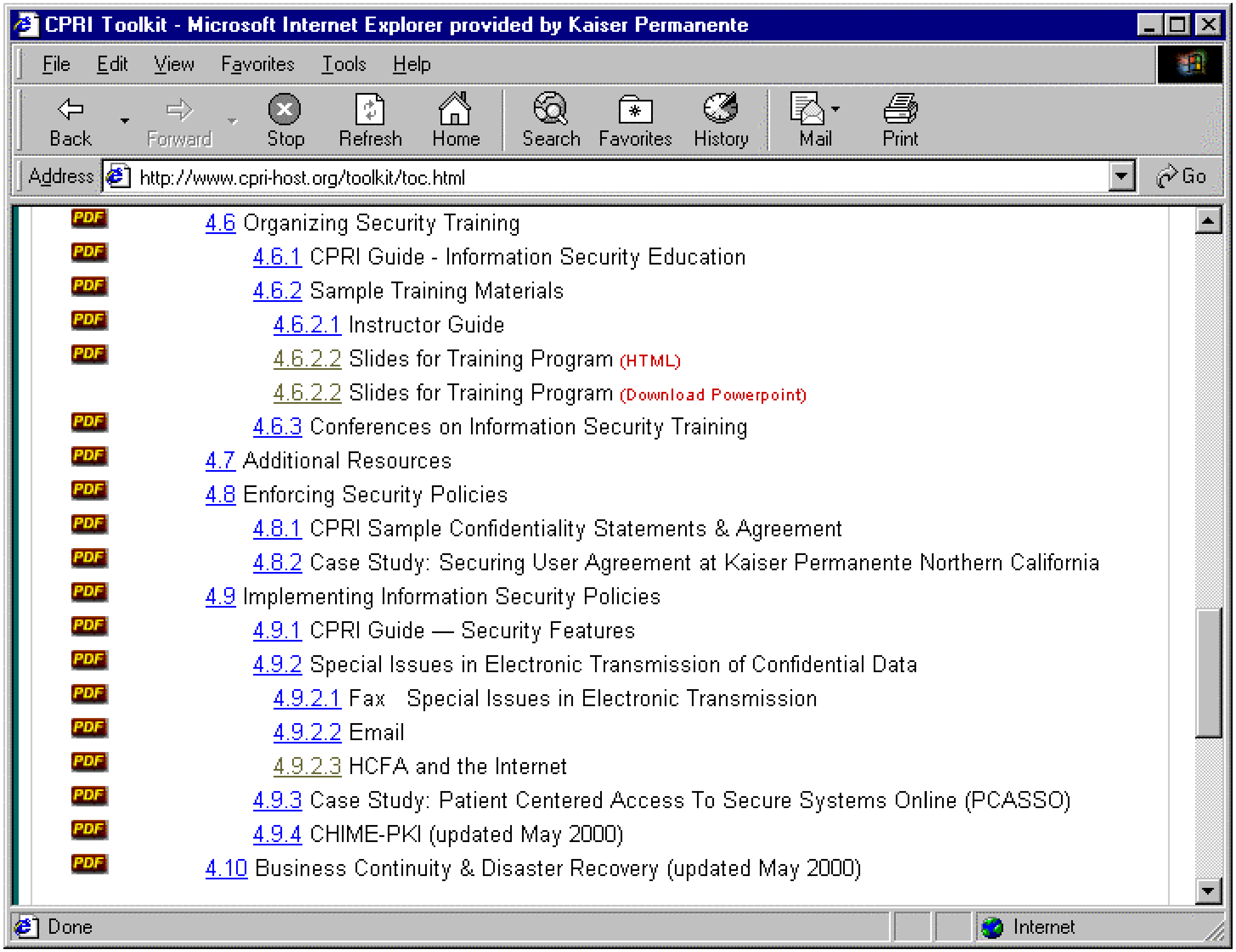
3.0 **Monitoring Laws, Regulations, and Standards**

Toolkit - Section 4.0 - 4.5.2



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
Done
Internet

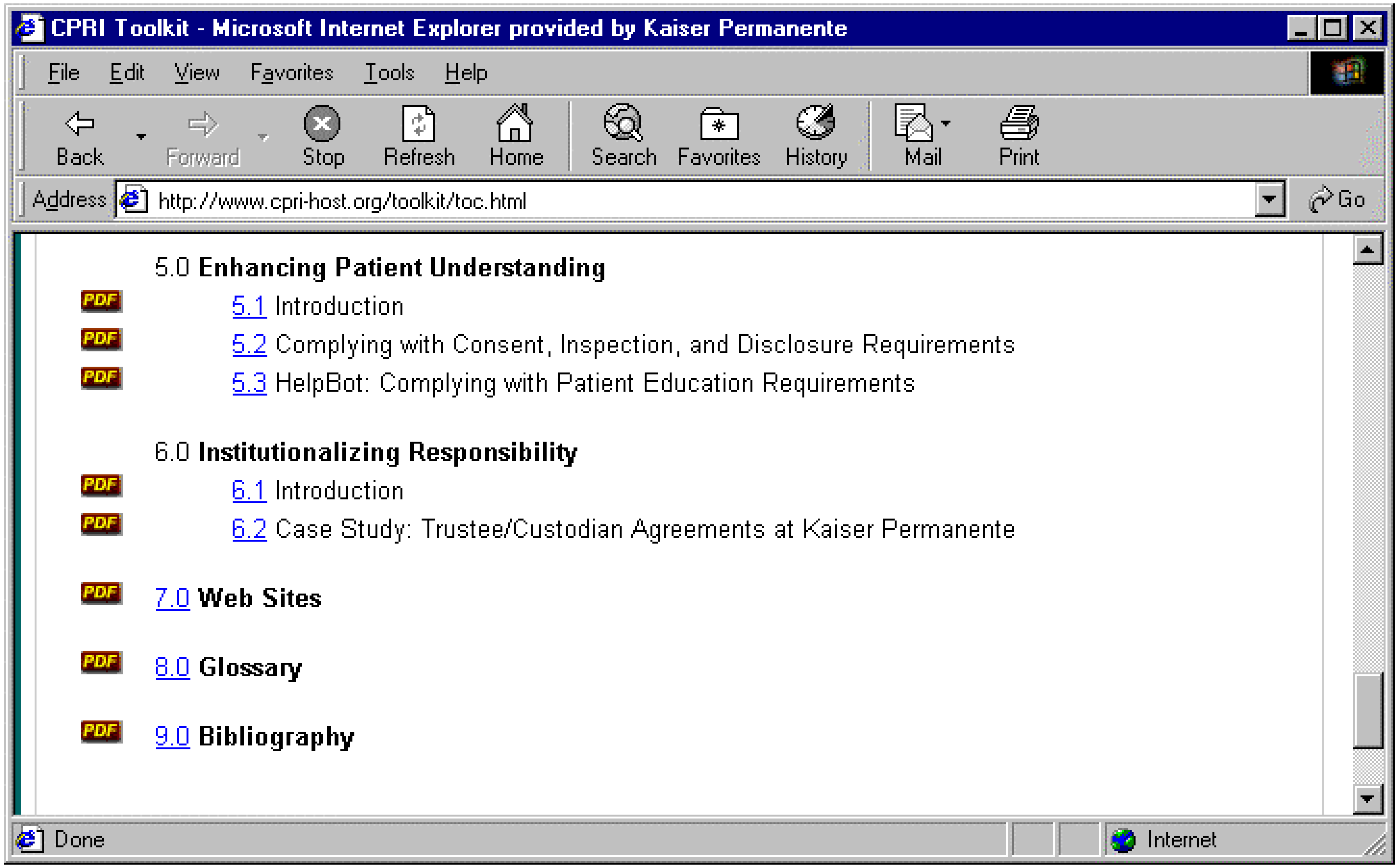
Toolkit - Section 4.6 - 4.10


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
Go
Done
Internet

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

- PDF 4.6 Organizing Security Training
  - PDF 4.6.1 CPRI Guide - Information Security Education
  - PDF 4.6.2 Sample Training Materials
    - PDF 4.6.2.1 Instructor Guide
    - PDF 4.6.2.2 Slides for Training Program (HTML)
    - 4.6.2.2 Slides for Training Program (Download Powerpoint)
  - PDF 4.6.3 Conferences on Information Security Training
- PDF 4.7 Additional Resources
- PDF 4.8 Enforcing Security Policies
  - PDF 4.8.1 CPRI Sample Confidentiality Statements & Agreement
  - PDF 4.8.2 Case Study: Securing User Agreement at Kaiser Permanente Northern California
- PDF 4.9 Implementing Information Security Policies
  - PDF 4.9.1 CPRI Guide — Security Features
  - PDF 4.9.2 Special Issues in Electronic Transmission of Confidential Data
    - PDF 4.9.2.1 Fax   Special Issues in Electronic Transmission
    - PDF 4.9.2.2 Email
    - PDF 4.9.2.3 HCFA and the Internet
  - PDF 4.9.3 Case Study: Patient Centered Access To Secure Systems Online (PCASSO)
  - PDF 4.9.4 CHIME-PKI (updated May 2000)
- PDF 4.10 Business Continuity & Disaster Recovery (updated May 2000)

Toolkit - Section 5-9



CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

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

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

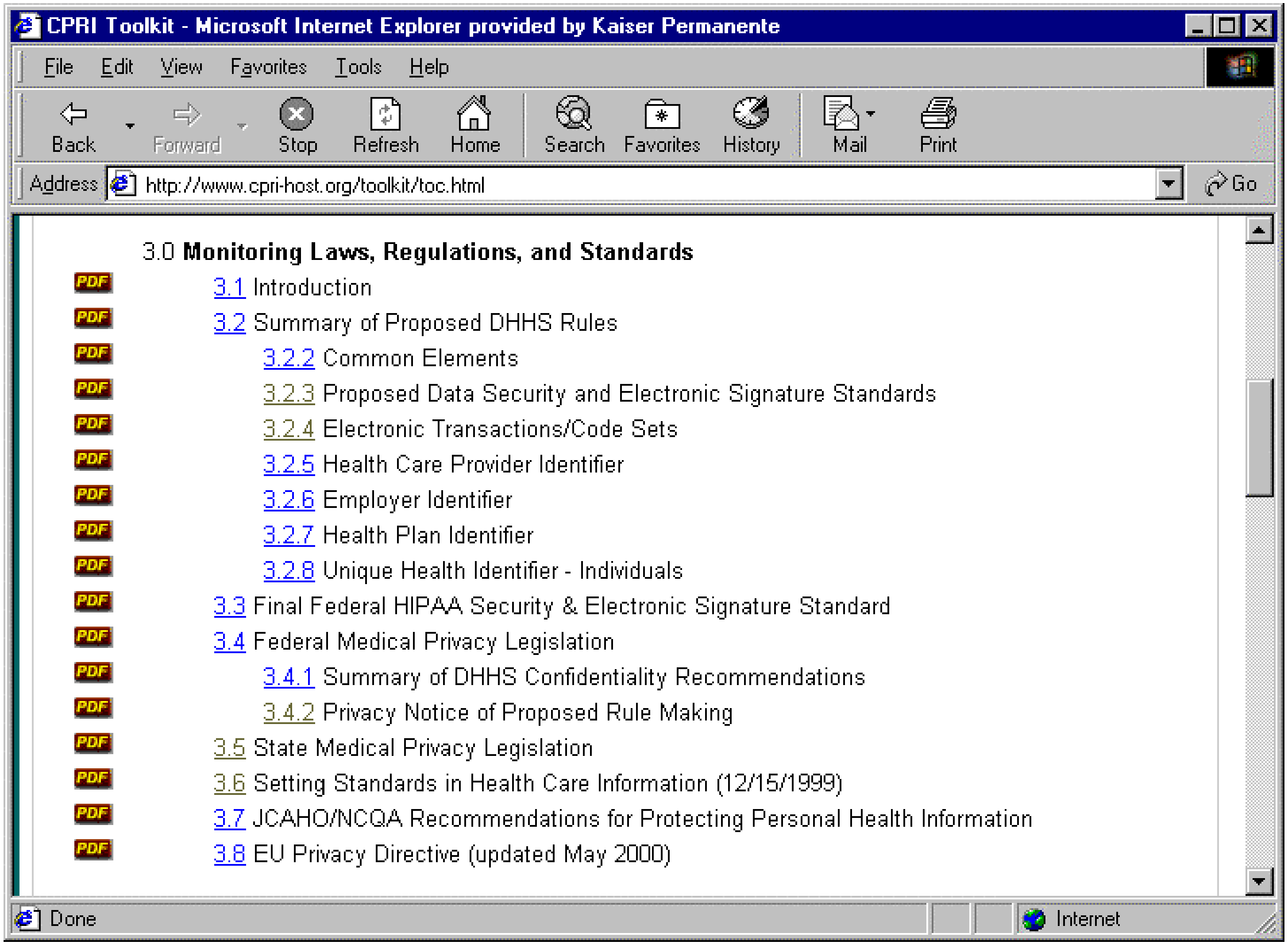
1. Deciding what to do

- *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

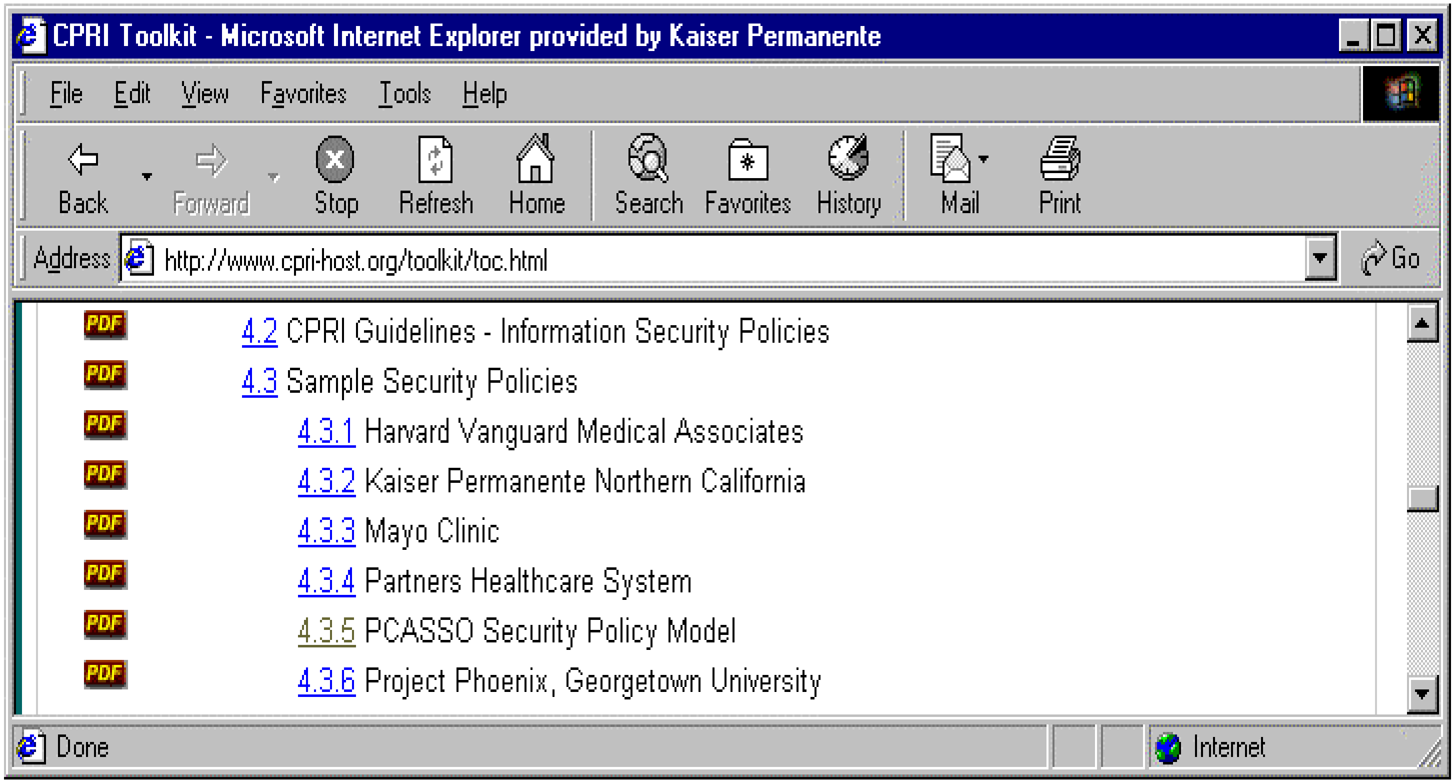


CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address
http://www.cpri-host.org/toolkit/toc.html
Go
Done
Internet

3.0 **Monitoring Laws, Regulations, and Standards**

PDF 3.1 Introduction
PDF 3.2 Summary of Proposed DHHS Rules
PDF 3.2.2 Common Elements
PDF 3.2.3 Proposed Data Security and Electronic Signature Standards
PDF 3.2.4 Electronic Transactions/Code Sets
PDF 3.2.5 Health Care Provider Identifier
PDF 3.2.6 Employer Identifier
PDF 3.2.7 Health Plan Identifier
PDF 3.2.8 Unique Health Identifier - Individuals
PDF 3.3 Final Federal HIPAA Security & Electronic Signature Standard
PDF 3.4 Federal Medical Privacy Legislation
PDF 3.4.1 Summary of DHHS Confidentiality Recommendations
PDF 3.4.2 Privacy Notice of Proposed Rule Making
PDF 3.5 State Medical Privacy Legislation
PDF 3.6 Setting Standards in Health Care Information (12/15/1999)
PDF 3.7 JCAHO/NCQA Recommendations for Protecting Personal Health Information
PDF 3.8 EU Privacy Directive (updated May 2000)

Information Security Policies


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
Done
Internet

PDF 4.2 CPRI Guidelines - Information Security Policies

PDF 4.3 Sample Security Policies

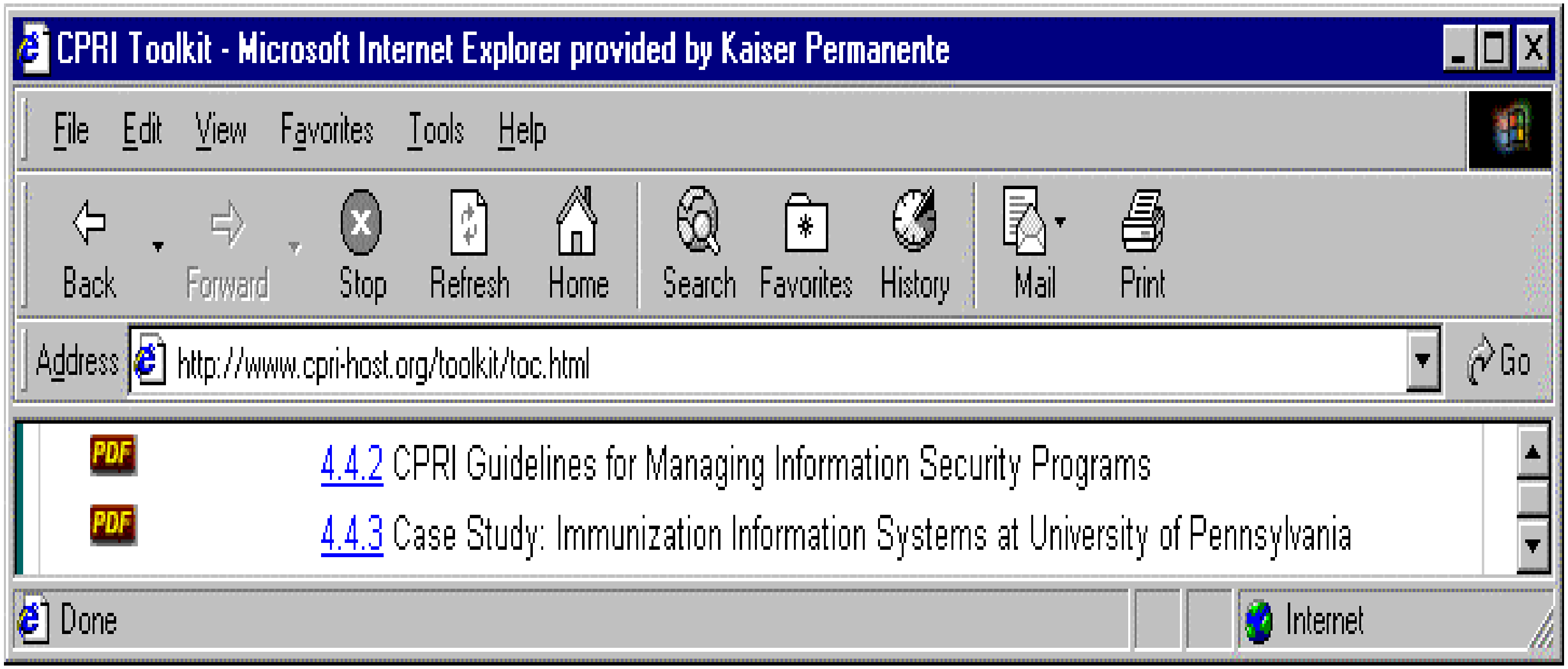
- PDF 4.3.1 Harvard Vanguard Medical Associates
- PDF 4.3.2 Kaiser Permanente Northern California
- PDF 4.3.3 Mayo Clinic
- PDF 4.3.4 Partners Healthcare System
- PDF 4.3.5 PCASSO Security Policy Model
- PDF 4.3.6 Project Phoenix, Georgetown University

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



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
Done
Internet

PDF 4.4.2 CPRI Guidelines for Managing Information Security Programs

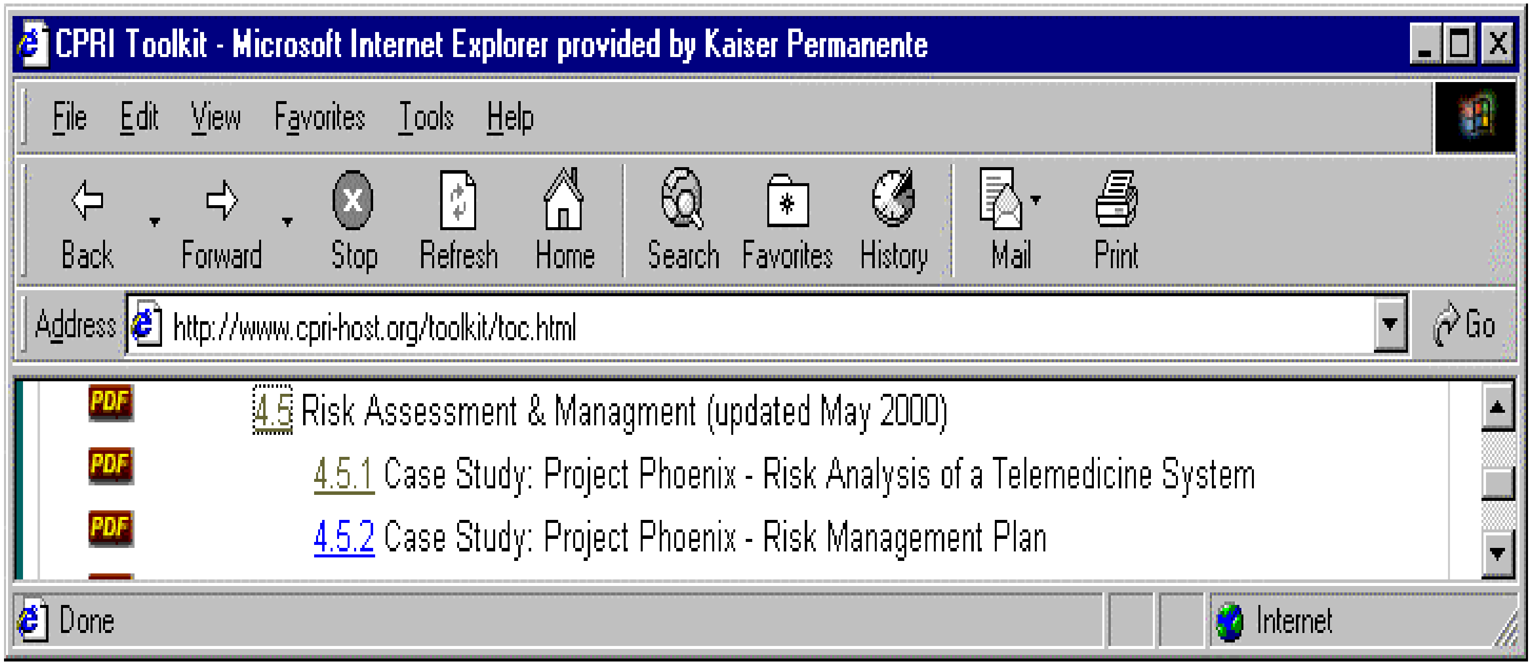
PDF 4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania

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



CPRI Toolkit - Microsoft Internet Explorer provided by Kaiser Permanente

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

PDF 4.5 Risk Assessment & Managment (updated May 2000)

PDF 4.5.1 Case Study: Project Phoenix - Risk Analysis of a Telemedicine System

PDF 4.5.2 Case Study: Project Phoenix - Risk Management Plan

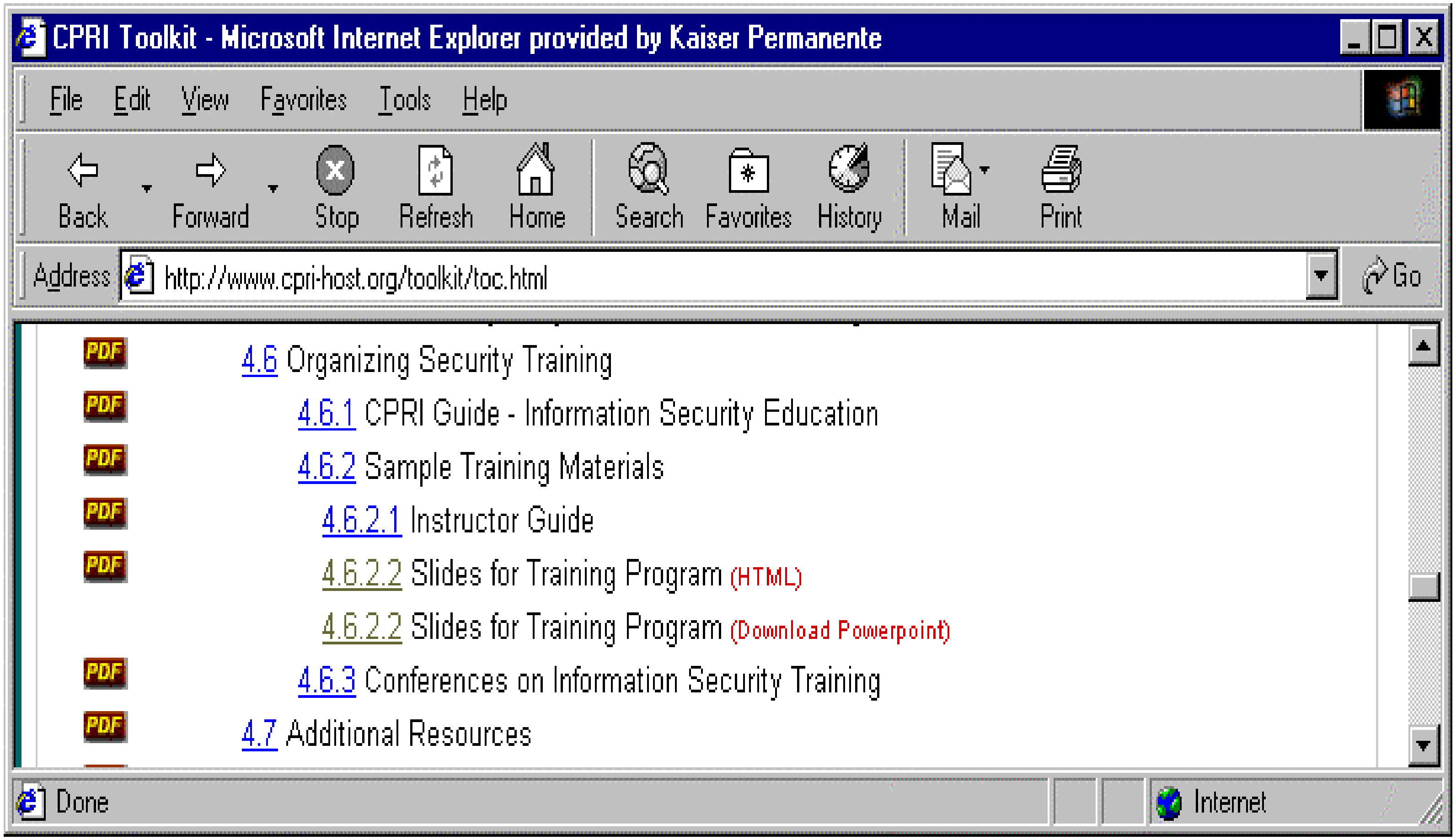
Done

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



http://www.cpri-host.org/toolkit/toc.html

PDF 4.6 Organizing Security Training

PDF 4.6.1 CPRI Guide - Information Security Education

PDF 4.6.2 Sample Training Materials

PDF 4.6.2.1 Instructor Guide

PDF 4.6.2.2 Slides for Training Program (HTML)

4.6.2.2 Slides for Training Program (Download Powerpoint)

PDF 4.6.3 Conferences on Information Security Training

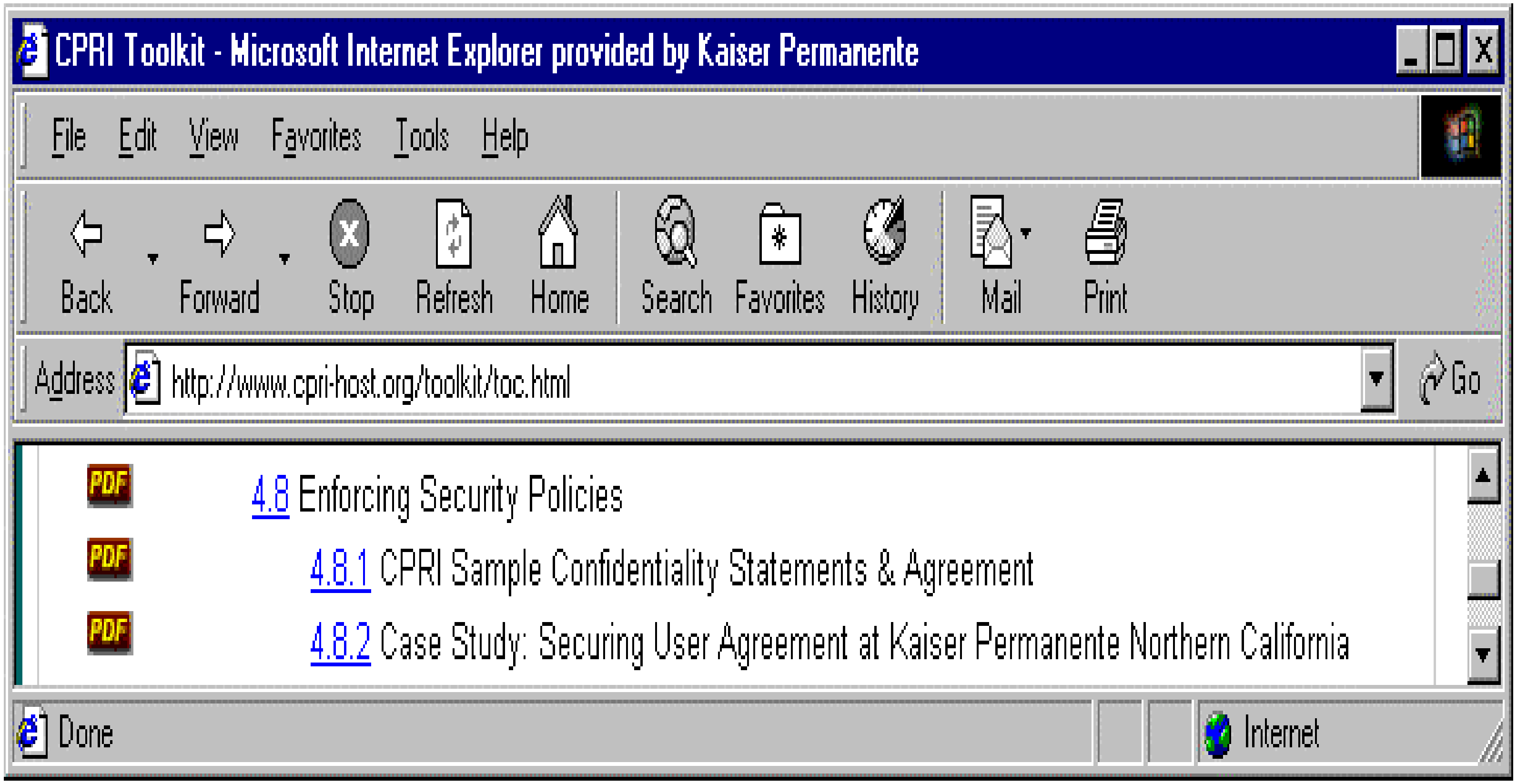
PDF 4.7 Additional Resources

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



http://www.cpri-host.org/toolkit/toc.html

4.8 Enforcing Security Policies

4.8.1 CPRI Sample Confidentiality Statements & Agreement

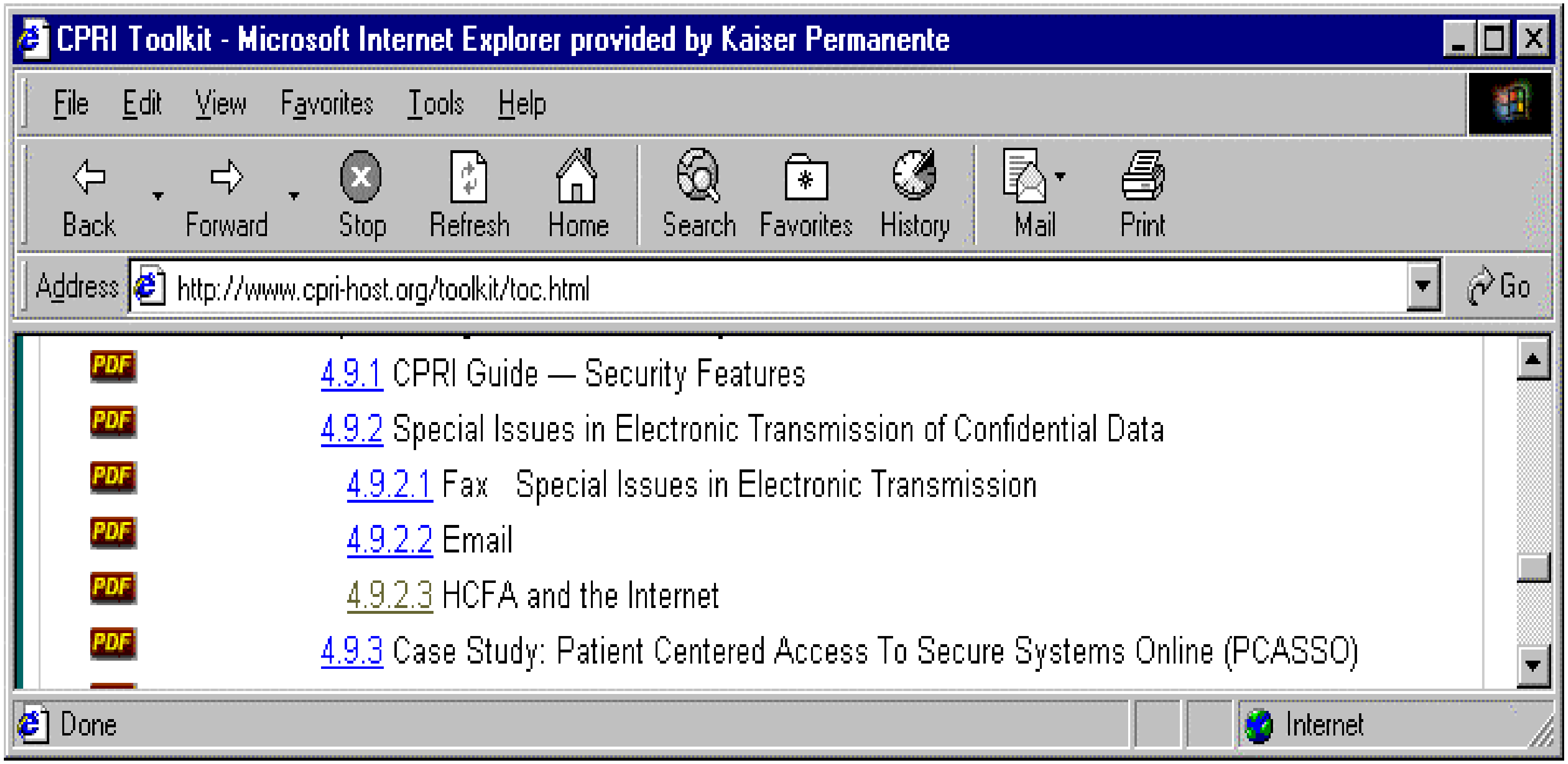
4.8.2 Case Study: Securing User Agreement at Kaiser Permanente Northern California

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


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
Go
Done
Internet

http://www.cpri-host.org/toolkit/toc.html

PDF 4.9.1 CPRI Guide — Security Features

PDF 4.9.2 Special Issues in Electronic Transmission of Confidential Data

PDF 4.9.2.1 Fax Special Issues in Electronic Transmission

PDF 4.9.2.2 Email

PDF 4.9.2.3 HCFA and the Internet

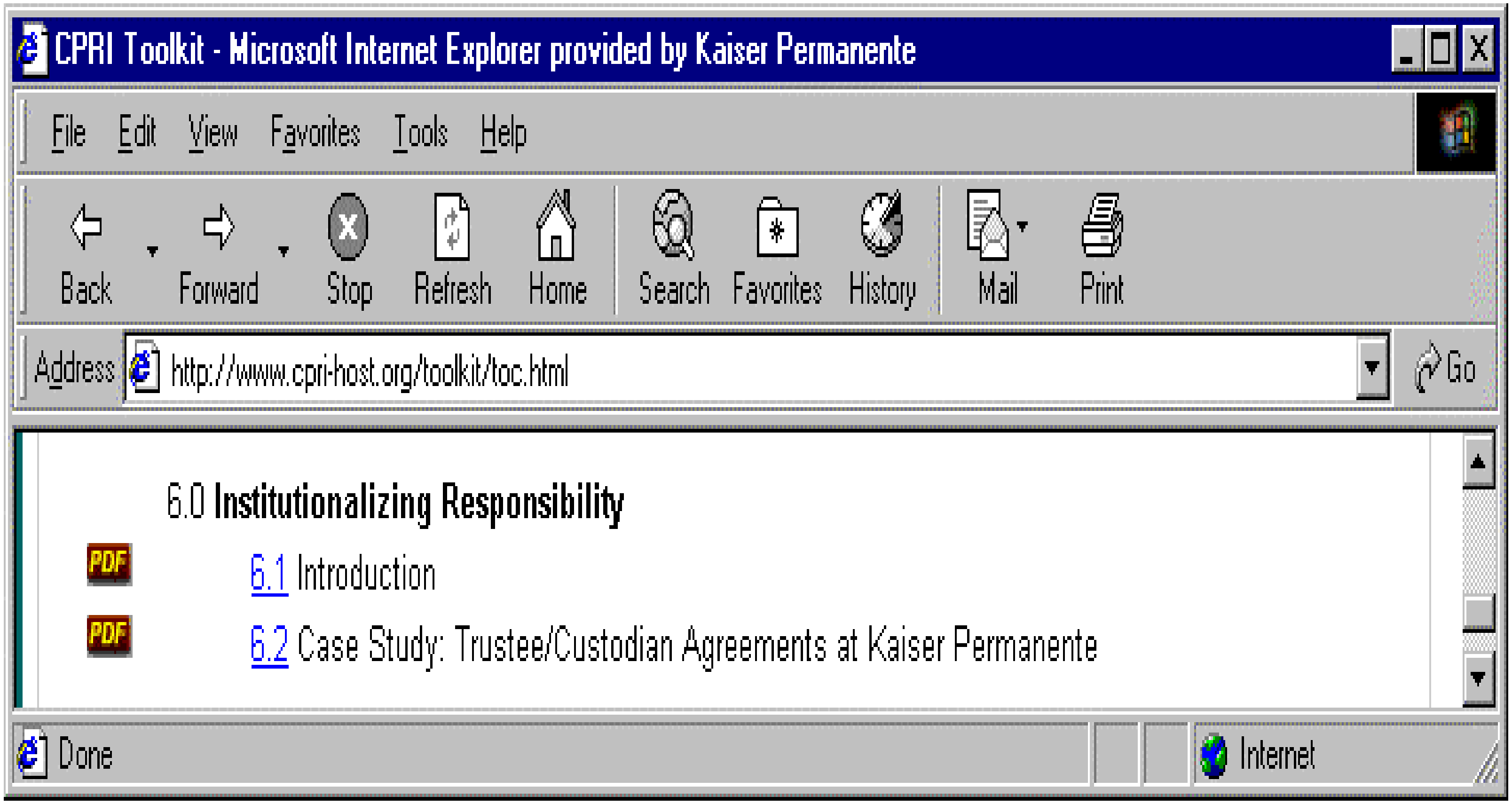
PDF 4.9.3 Case Study: Patient Centered Access To Secure Systems Online (PCASSO)

Toolkit & Critical Steps

7. Institutionalizing Responsibility

- Kaiser’s Trustee-Custodian Agreement

Institutionalizing Responsibility



http://www.cpri-host.org/toolkit/toc.html

6.0 **Institutionalizing Responsibility**

6.1 Introduction

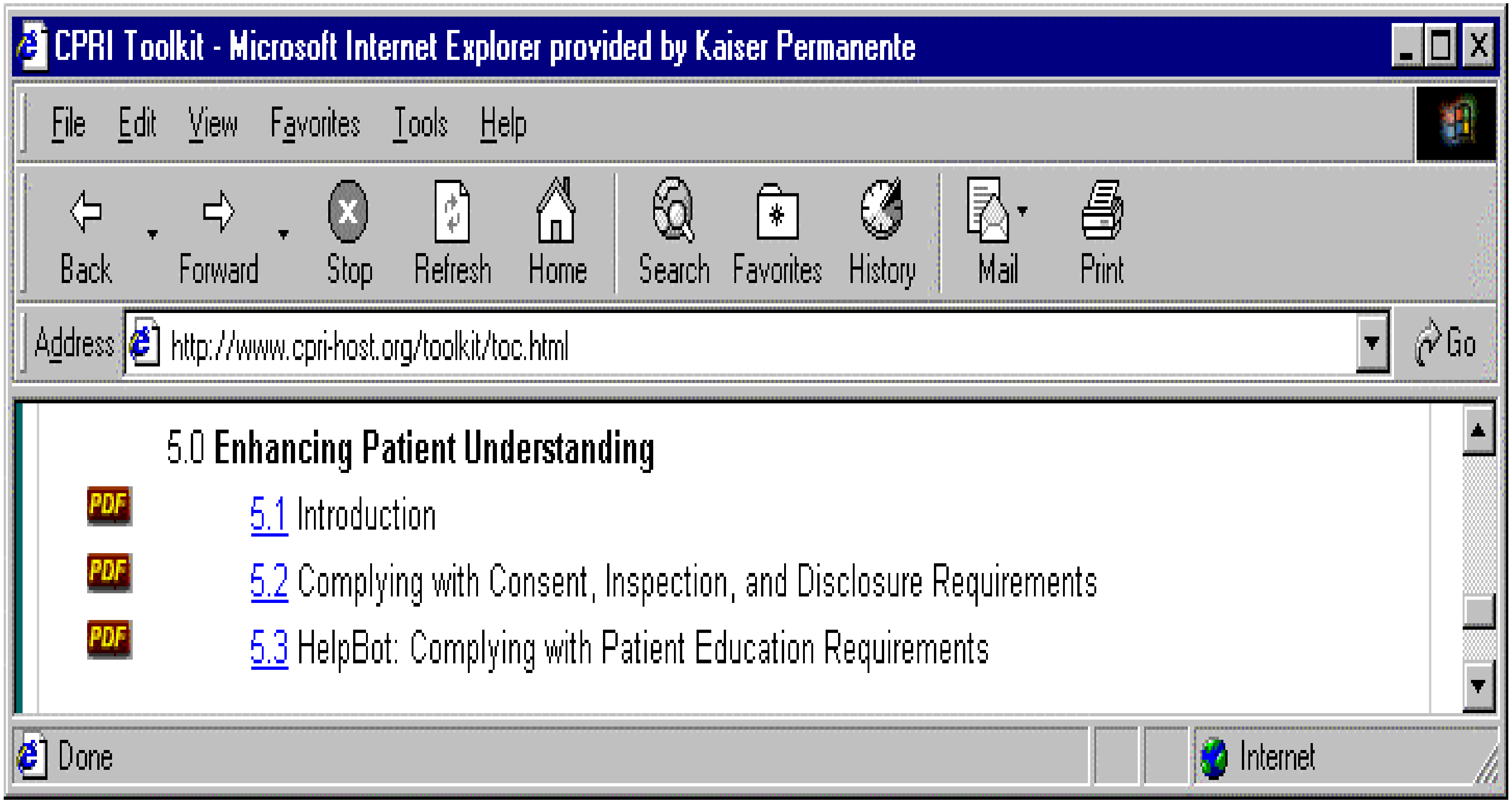
6.2 Case Study: Trustee/Custodian Agreements at Kaiser Permanente

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


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
Go
Done
Internet

http://www.cpri-host.org/toolkit/toc.html

5.0 Enhancing Patient Understanding

PDF 5.1 Introduction

PDF 5.2 Complying with Consent, Inspection, and Disclosure Requirements

PDF 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 EarlyView™

target your weaknesses with this powerful self-evaluation tool

HIPAA Self-evaluation Tools

» Privacy HEVp

» Security HEVs

NCHICA

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*Ô *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*****Ô** ***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.

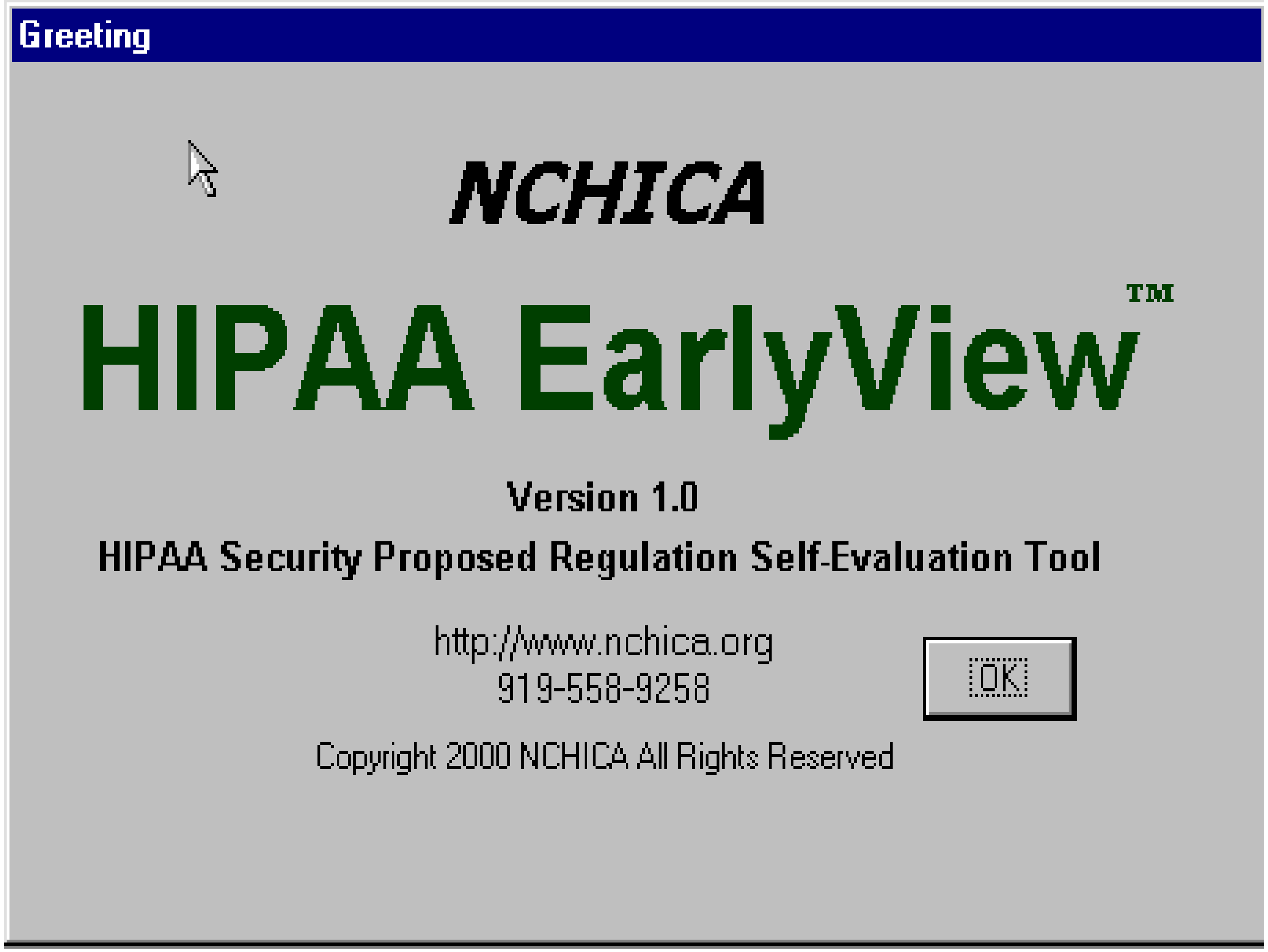
• HIPAA EarlyView™ Security is intended for health plans, provider organizations, clearinghouses, and public agencies.

• 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*Ô *Security?*

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



NCHICA

HIPAA EarlyView™

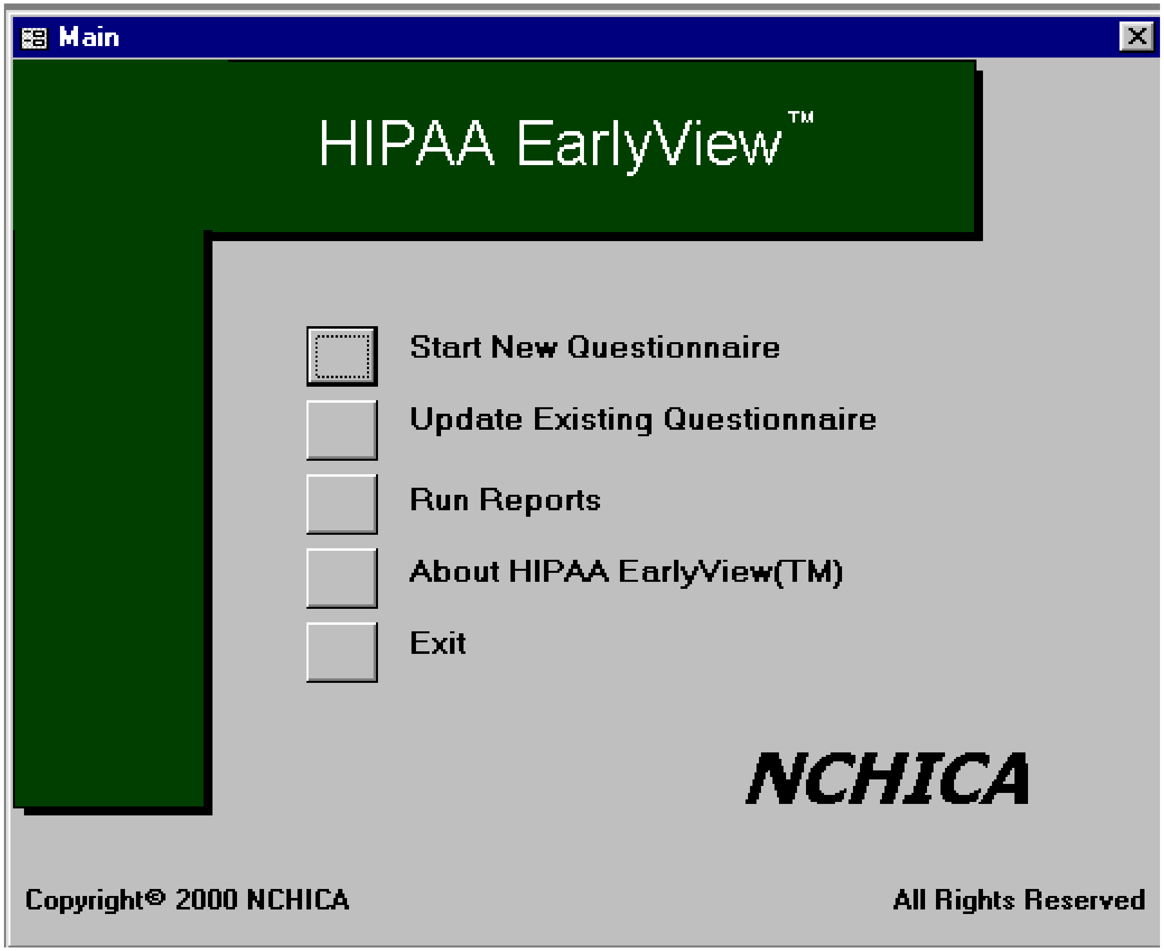
Version 1.0

HIPAA Security Proposed Regulation Self-Evaluation Tool

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

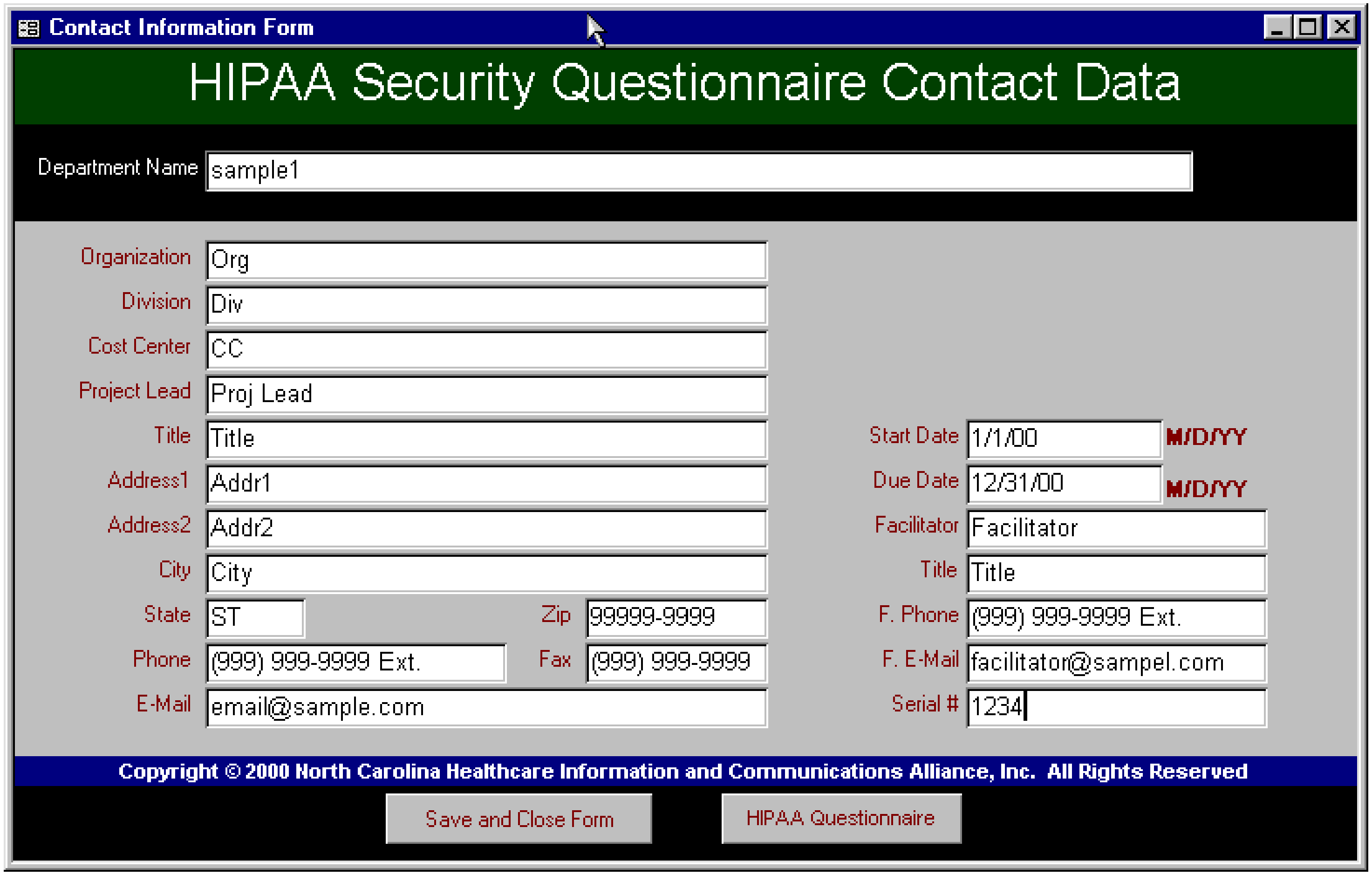
Copyright 2000 NCHICA All Rights Reserved

Main Menu



Main
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



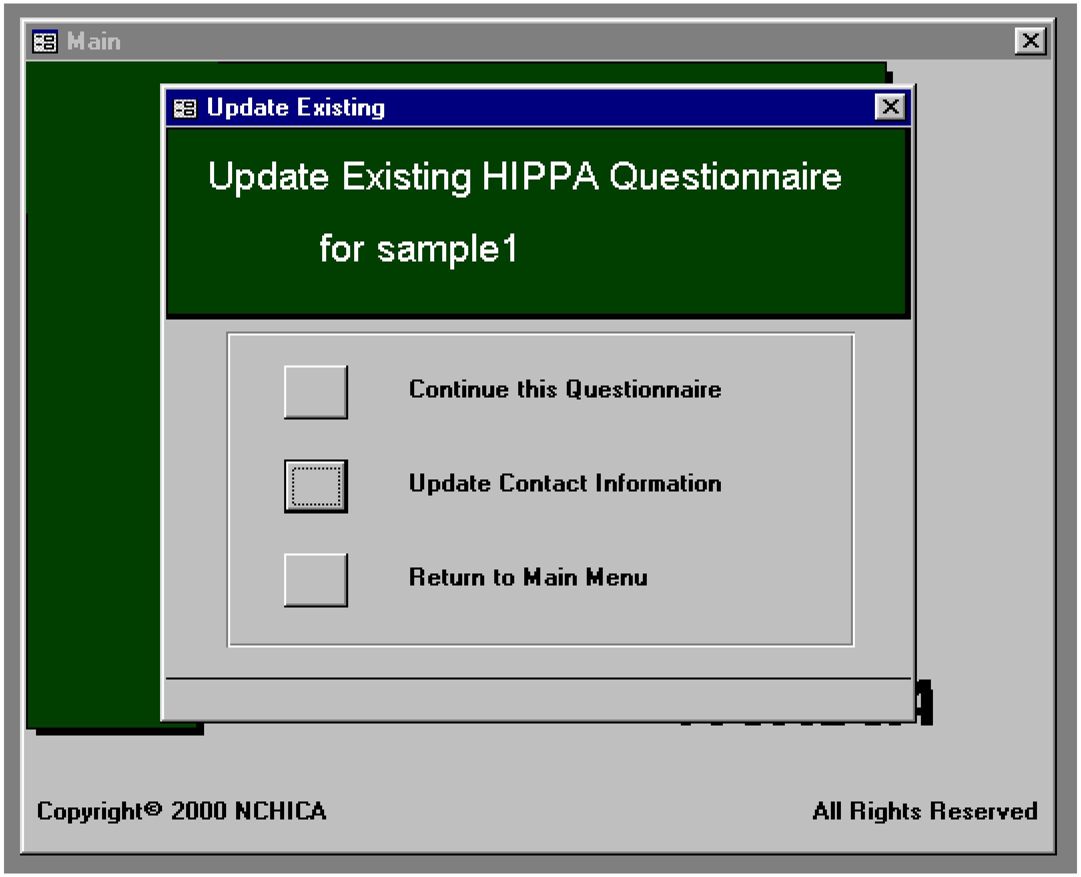
HIPAA Security Questionnaire Contact Data

Department Name: sample1

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

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

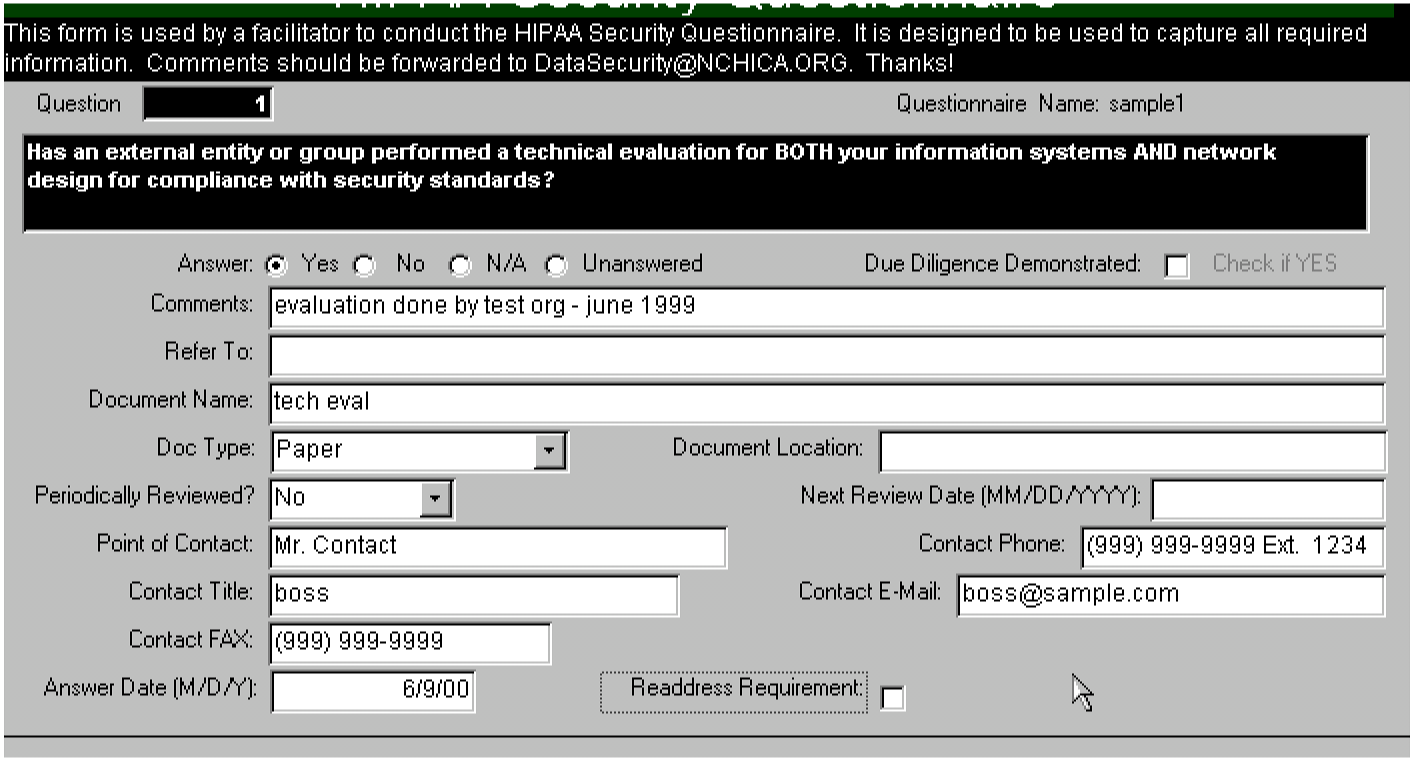
Update Questionnaire Menu



Update Existing HIPPA Questionnaire

for sample1

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

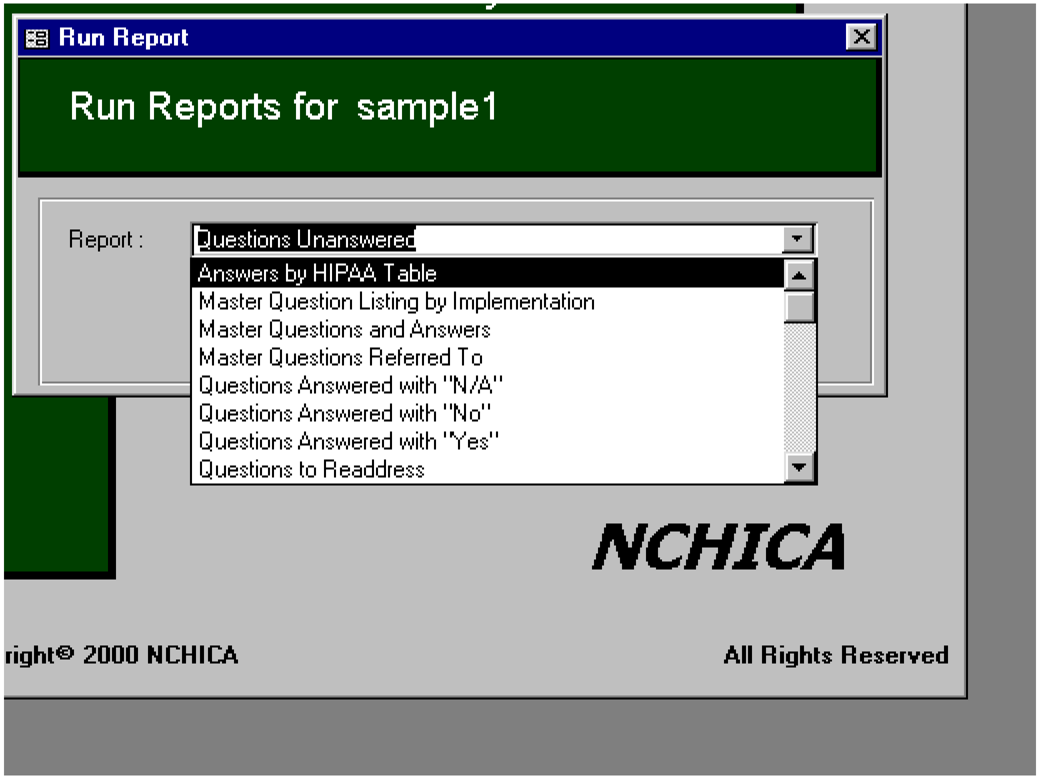
Contact E-Mail: boss@sample.com

Contact FAX: (999) 999-9999

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

Readdress Requirement: □

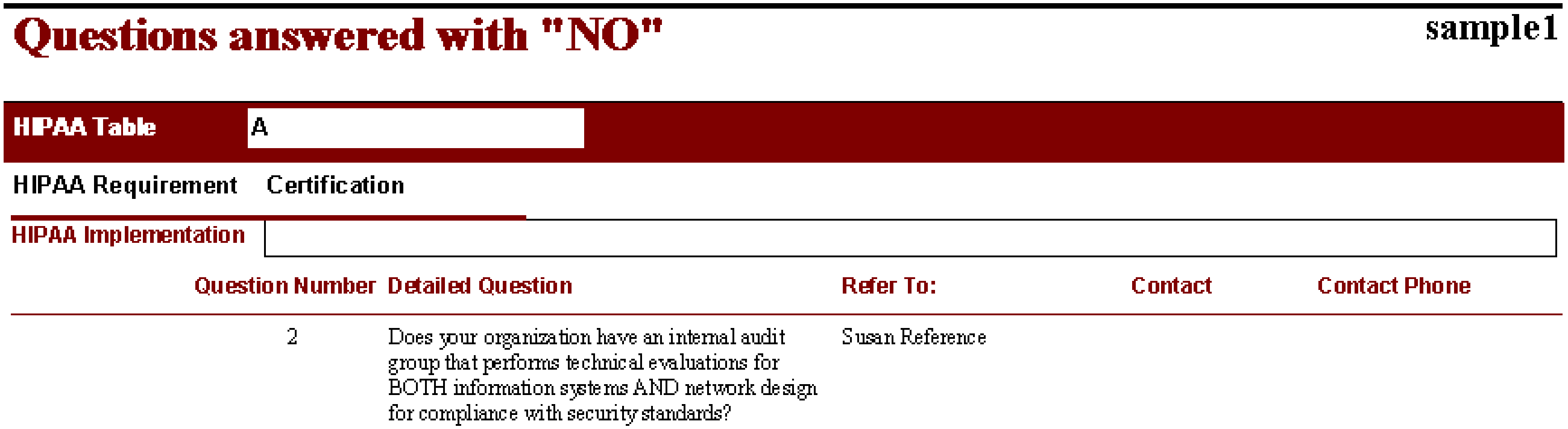
Report Menu



Report : Questions Unanswered

- Answers by HIPAA Table
- Master Question Listing by Implementation
- Master Questions and Answers
- Master Questions Referred To
- Questions Answered with "N/A"
- Questions Answered with "No"
- Questions Answered with "Yes"
- Questions to Readdress

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		

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

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)

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

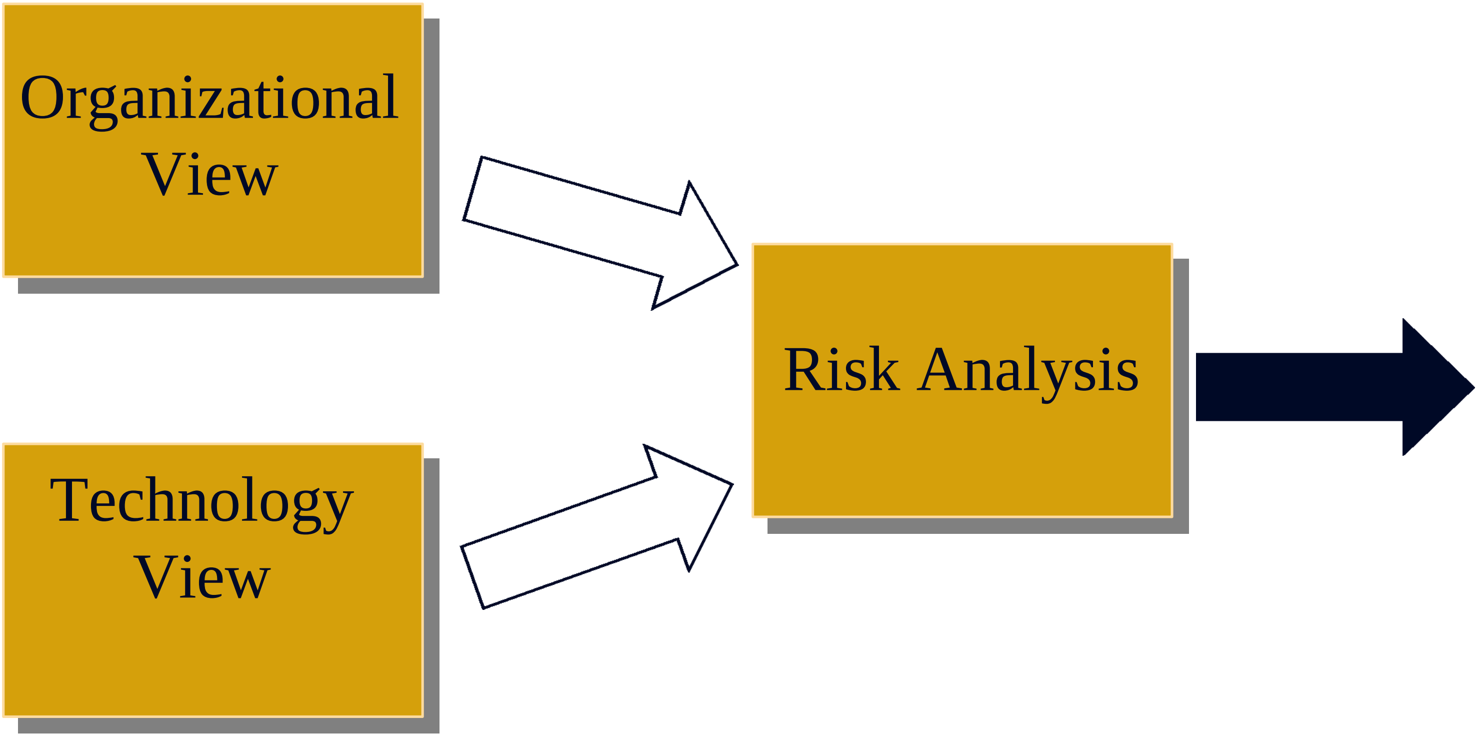
Why a Self Directed Approach?

- 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
  - http://www.cert.org/archive/pdf/01tr020.pdf

- Printed guide & the CD-ROM is $400

Generally Accepted System Security Principles (GASSP)

- The International Information Security Foundation (I^{2}SF) - 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
  - http://66.129.1.101/top20.htm
- 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

http://snip.wedi.org/public/articles/index.cfm?cat=6

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

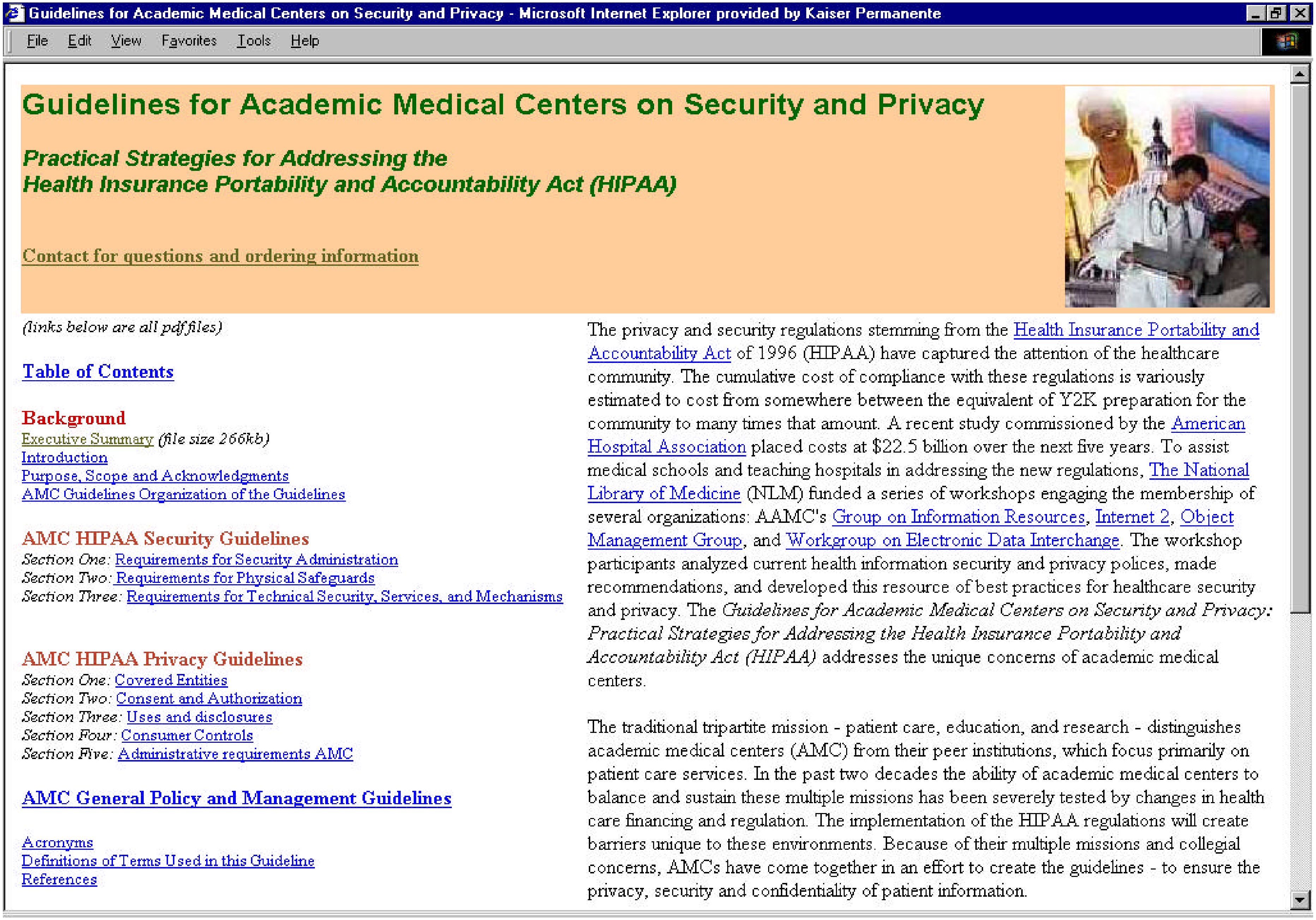
- Association of American Medical Centers
- Internet 2
- National Library of Medicine
- Object Management Group

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 - Microsoft Internet Explorer provided by Kaiser Permanente
File
Edit
View
Favorites
Tools
Help

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.

PSN HIPAA Calculators™

- The PSN HIPAA Calculators™ provide you with free - real-time - initial consultations of your organization's compliance with the HIPAA 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 HIPAA 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 HIPAA Calculator™ will take that answer into account when preparing the Report.
- http://www.privacysecuritynetwork.com/healthcare/hipaa/

Thank you!