



# The Coalition of Voluntary Mental Health Agencies, Inc

## HIPAA Security Tools – Order Form

**Please return this completed form along with check made payable to 'The Coalition':**

The Coalition of Voluntary Mental Health Agencies  
Attn: Karyn Krampitz  
90 Broad St, 8<sup>th</sup> Fl  
New York, NY 10004

**Information Flow Analysis and Risk Assessment CD**

(see following pages for a listing of the documents included on the CD)

\_\_\_\_\_ **Members \$50**                      \_\_\_\_\_ **Non-Members \$100**

**HIPAA Security Policy Templates CD**

(see following pages for a listing of the documents included on the CD)

\_\_\_\_\_ **Members \$50**                      \_\_\_\_\_ **Non-Members \$100**

**HIPAA Security Training Awareness Manual**

(see following pages for a listing of the documents included on the CD)

\_\_\_\_\_ **Members \$50**                      \_\_\_\_\_ **Non-Members \$100**

**Total Enclosed:** \_\_\_\_\_

**Organization Name:** \_\_\_\_\_

**HIPAA Security Officer:** \_\_\_\_\_

**Phone Number:** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

**Ship to:** \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

If you have any questions, please contact Karyn Krampitz at [kkrampitz@cvmha.org](mailto:kkrampitz@cvmha.org) or 212-742-1600 x 103.

## List of Documents

### CVMHA Information Flow Analysis and Risk Analysis Seminar October 29, 2004

#### **0.1 List of Documents.pdf**

This list identifies the various documents provided with this seminar, and identifies any special printing needs or requirements.

#### **0.2 IFA and RA Process.pdf**

A list of the steps of Information Flow Analysis and Risk Assessment in order, as a simple overall guide to the process.

#### **0.3 Security Rule CFR.pdf**

The regulation text, including preamble and comments. The actual regulation text is at the end and is only a few pages, but all the other discussion can be enlightening if you have a question.

#### **0.4 2004-07 RiskAnalysis.pdf**

Working Draft 1.0 of the WEDI-SNIP *Risk Analysis White Paper* (will be the final draft). This is an excellent guidance document with suggested issues to consider for each section of the regulations.

#### **1.1 CVMHA HIPAA IFA/RA Pres.pdf**

The presentation PowerPoint for the entire combined IFA/RA session, in a PDF file format for easy, automatic printing with three slides per page.

#### **1.2 SP800-14(GAPP).pdf**

The National Institute of Standards and Technology (NIST) Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*. This is an excellent overall guide to information security.

#### **1.3 HIPAA Security Summary.xls**

An Excel spreadsheet that summarizes the Security regulation text into a set of questions. This summary is useful for an overall view of readiness for HIPAA compliance.

#### **1.4 SP800-30-RevA-draft.pdf**

NIST Special Publication 800-30, a revised draft of *Risk Management Guide for Information Technology Systems*. Chapters 3 and 4 are most relevant to the work at hand.

#### **1.5 Interview Questionnaire.doc**

A set of questionnaires to be used as interview tools for each program and system, as a Word document that can be printed and used and/or filled out upon completion of the interviews.

#### **1.6 Systems Security Qnnre.xls**

A subset of the questions listed in the HIPAA Security Summary, specific to systems, prompting for identification of Vulnerabilities, Threats, and Controls. This document can be used as a questionnaire tool and/or worksheet for developing information.

#### **1.7 SP800-26 Self Assessmnt.pdf**

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides a detailed questionnaire for system security assessment as part of the Risk Assessment. Printing it at two pages per sheet is a good idea – it is just under 100 pages.

#### **1.8 Info Flow Descriptions.doc**

These sample descriptions show how relatively simple and relatively complex information flows might be written up. These descriptions may be used as templates if desired.

#### **1.9 Info Flow Diagrams.doc**

These are sample diagrams of the descriptions in the previous document. The diagrams are created entirely using the tools in Microsoft Word and can be edited and used as templates. (Go to View > Toolbars > Drawing to enable your drawing toolbar)

#### **2.1 CMS Risk Assmt Methodgy.pdf**

The *CMS Risk Assessment Methodology* represents one interpretation of how to perform a risk assessment based on the NIST process. This document includes useful guidelines and procedures.

#### **2.2 CMS Risk Assmt Template.doc**

The *CMS Risk Assessment Template* is an editable Word document that can be modified and used for Risk Assessments if desired, or its elements can be incorporated into your own template.

#### **2.3 CMS Info SecurityLevels.doc**

This brief document describes the standards CMS uses in determining the level of security of information for various types of information.

#### **2.4 CMS Threat ID Resource.pdf**

The *CMS Threat Identification Resource* is a valuable tool to help you discover and identify the threats that could result in information security incidents. This can be printed 2 pages to a sheet.

#### **2.5 CMS Risk Safeguards.pdf**

*CMS Information Security Acceptable Risk Safeguards* provides information about the measures that can be taken to deal with various threats at different security levels. This is best printed 2 pages to a sheet.

#### **2.6 Risk Determination Template.doc**

The *Risk Determination Template* is used to collect and present the information gathered in the course of Steps 1 through 7 of the NIST Risk Assessment procedure, and is focused on systems.

#### **2.7 Organiz'n Control Plan.doc**

The *Organization Security Control Plan* collects the information about the various systems and presents the chosen control measures to be implemented at an organization level, with justification as necessary.

# Table of Contents – HIPAA Security Policies

## Introduction

## How to Use These Policy Templates

1. Workforce Compliance with HIPAA Security Provisions
  2. Information Security Management Process
  3. Information Security Sanction Policy
  4. Assigned Security Responsibility
  5. Workforce Authorization and Clearance
  6. Termination Procedures
  7. Information Access Management
  8. Information Security Awareness and Training
  9. Information Security Incident Procedures
  10. Data Backup Policy
  11. Contingency Plan
  12. Information Security Evaluation
  13. Contracts and Memoranda of Understanding Regarding Electronic Protected Health Information
  14. Facility Access Controls
  15. Use of Cell Phones
  16. Workstation Use Policy
  17. Electronic Information Device and Media Controls
  18. Technical Access Control and Authentication
  19. Perimeter Security Policy
  20. Remote Access Policy
  21. Data Encryption Policy
  22. Information Systems Audit Controls
  23. Data Integrity Policy
  24. Transmission Security Policy
  25. Security Requirements for the Group Health Plan
  26. Documentation for HIPAA Security Rule Requirements
  27. Information Disposal Policy
- Appendix: Glossary of Terms**

## Also included on the CD:

HIPAA Final Security Regulations Matrix with Preamble Notes

NIST HIPAA Guides

NIST Introductory Resource Guide for Implementing the HIPAA Security Rule – Draft

# **Table of Contents – HIPAA Security Awareness Training**

## **Training Administrator's Information**

**INTRODUCTION**

**HOW TO USE THESE MATERIALS**

**TABLE OF MODULES AND AUDIENCES**

**QUIZ: ADMINISTRATOR'S VERSION**

**APPENDIX: GLOSSARY OF TERMS**

**QUIZ: HOW WELL DO YOU UNDERSTAND INFORMATION SECURITY?**

## **HIPAA Security Rule Awareness Training**

**MODULE 1. OVERVIEW OF HIPAA AND THE SECURITY RULE**

**MODULE 2. SITE SECURITY AND EMERGENCY PLANS**

**MODULE 3. PHYSICAL ACCESS TO WORKSTATION AREAS**

**MODULE 4. OBTAINING AND USING ACCESS TO ELECTRONIC INFORMATION**

**MODULE 5. PASSWORDS AND GUARDING YOUR IDENTITY**

**MODULE 6. ACCEPTABLE USE OF COMPUTERS AND THE INTERNET**

**MODULE 7. AUDITING OF COMPUTER ACTIVITY**

**MODULE 8. GUARDING AGAINST MALICIOUS SOFTWARE**

**MODULE 9. DANGERS OF INSTALLING YOUR OWN SOFTWARE**

**MODULE 10. ATTACHING DEVICES TO YOUR NETWORKS (INCLUDING WIRELESS ACCESS POINTS)**

**MODULE 11. PREVENTING OTHERS FROM VIEWING YOUR WORKSTATION**

**MODULE 12. HOW TO DEAL WITH SECURITY INCIDENTS**

**MODULE 13. BACKING UP HEALTH INFORMATION**

**MODULE 14. USE OF CELL PHONES, CAMERAS, AND PICTURE PHONES**

**MODULE 15. WHAT IF YOUR JOB CHANGES?**

**MODULE 16. SENDING HEALTH INFORMATION OVER THE INTERNET**

**MODULE 17. ACCESSING HEALTH INFORMATION FROM HOME**

**MODULE 18. USING A LAPTOP THAT CONTAINS HEALTH INFORMATION**

**MODULE 19. PERSONAL DIGITAL ASSISTANTS AND HEALTH INFORMATION**

**MODULE 20. DISPOSING OF OR HANDING DOWN A PC OR PDA**

**MODULE 21. TRANSPORTING DISKS, CDS, AND TAPES HOLDING PHI**

**MODULE 22. DISPOSING OF PORTABLE MEDIA (CDS, DISKS, & DRIVES)**

**APPENDIX: GLOSSARY OF TERMS**