Volume

1

UC DAVIS HEALTH SYSTEM

HIPAA Security Compliance Workbook

# Multi – User Guide

UC DAVIS HEALTH SYSTEM

# HIPAA Security Compliance Workbook Guide

# Table of Contents

# INTRODUCTION

The UCDHS HIPAA Security Compliance Workbook has been prepared to support the UCDHS HIPAA Security Initiative. For this phase of the Initiative, each system must be brought into compliance with the HIPAA security regulations by the April 20 deadline. The workbook has been created to assist users in implementing, upgrading and documenting their computing practices in order to achieve HIPAA Security Compliance.

**PURPOSE**

The Workbook is intended to be a "lowest common denominator" guide for users to achieve and maintain satisfactory compliance with the HIPAA security regulations. The "entry level" solutions and procedures presented are not intended to be adopted in their entirety by all users. Many users will have alternative processes, procedures and systems in place that adequately meet the objectives of various sections in the Workbook. In those cases, users are certainly free to continue using the alternative, equivalent procedures. The Workbook can serve as a useful vehicle for high-level, standardized documentation of the various alternative procedures actually employed; a "check-off sheet" to ensure that all required areas have been considered.

**ADDITIONAL HIPAA SECURITY REQUIREMENTS**

**In addition to the Workbook** material, there are several other HIPAA requirements that are being dealt with at the institutional and UC-wide level. You may be contacted from time to time to participate in those initiatives. For example, HIPAA regulations require that all individuals who use systems that contain ePHI receive periodic training on security awareness. The UCDHS Compliance and Security Offices are preparing training materials. These will be distributed to you at a later date.

**AUDIENCE**

The intended audiences for the Workbook are the UCDHS faculty, staff and students. Many of the services and solutions that are presented in the Workbook are available primarily or exclusively for use on UCDHS equipment or by UCDHS employees and faculty.

## Workbook Organization

The Workbook is composed of nine major sections; each covers a broad area of security requirements. The intent has been to "roll-up" the security requirements into a small number of unified sections. In the process, no attempt has been made to adhere to the order of requirements within the original regulations. Users who wish to view the detailed HIPAA Security regulations will find online references to them in the Workbook Appendix.

### MULTI-USER SYSTEMS: ADDITIONAL REQUIREMENTS

This version of the Workbook is intended primarily to document HIPAA Security compliance for Multi-User systems. That is, systems that support multiple user accounts and are routinely used by several individuals. Since the potential risk of unauthorized disclosure may be greater for such systems, HIPAA regulations require that additional safeguards be implemented. Section 9 of the Workbook presents the additional requirements and Standard compliance procedures.

### FORMAT

Most Sections contain three subsections:

1. REQUIREMENT. The relevant HIPAA security requirements that apply to the section are briefly itemized and discussed.
2. STANDARD. This subsection presents at least one "acceptable" solution (by UCDHS standards) to the requirements. The primary intent is to provide the average user with at least one simple method of meeting the relevant compliance requirements.
3. EQUIVALENT ALTERNATIVE SOLUTION. Many users will not adopt the Standard Solution, as they have alternative (no doubt better) methods already in place. They should document their alternative solution in this subsection.
4. Optional LOG SHEETS. In those cases where routine documentation of monitoring and maintenance activities is required, basic Log Sheets are provided for that purpose. The actual Log sheets can be used to maintain the required documentation, or they can serve as a basic template for developing alternative documentation procedures.

## GENERAL INSTRUCTIONS

**If you have received this workbook** as part of the UCDHS HIPAA Security Compliance Initiative, you should have also received an email summary of the results of the recent Compliance Survey Questionnaire. The summary lists those areas where the System is in compliance and those Workbook sections that require further security improvements. Even though the System may not need to have all the Workbook sections completed in order to achieve compliance, it is a good idea to do so anyway, since the Workbook can serve as a single, standardized source of documentation for future reference.

**Step-By-Step Instructions**.

1. System administrators should complete Sections 1 - 9 of the Workbook.
2. If any of the manual Log Sheets that are included in the Workbook will be used to document system maintenance activities, they should be prepared for each system listed in Section 1. The Logs should be distributed to the individuals who will actually be performing the maintenance activities.
3. Shortly prior to April 20, 2005 you will receive a brief Certification Document via email. By completing the Certification and returning it to the designated address, you will acknowledge your compliance with the HIPAA Security requirements.

If you have questions, please contact one of the following:

General Questions or Questions concerning the HIPAA Security Regulations
Email: Hippa.security@ucdmc.ucdavis.edu
Phone: 916-703-6591

Technical Questions regarding System hardware or software
UCDHS Customer Support Center
Phone: 734-HELP

## SECTION 1: Catalog of Systems

List all systems that are covered by this Workbook:
(Use additional copies of this page if necessary)

1. Asset Number assigned by UCDHS Security Office:

System Identification Number (serial number, UC Property Number, etc.):

System Description (Dell PC, IBM server, etc.):

System Location:

2. Asset Number assigned by UCDHS Security Office

System Identification Number (serial number, UC Property Number, etc.):

System Description (Dell PC, IBM server, etc.):

System Location:

3. Asset Number assigned by UCDHS Security Office

System Identification Number (serial number, UC Property Number, etc.):

System Description (Dell PC, IBM server, etc.):

System Location:

**Responsible Party**

This Workbook has been completed by (name/title):

## SECTION 2: Physical Security

### Requirements

1. Systems should be located in physically secure locations, whenever possible. A secure location would minimally be defined as one that is not routinely accessible to the public, particularly if authorized personnel are not always available to monitor security.
2. Secure locations must have physical access controls (Card Key, door locks, etc.) that prevent unauthorized entry, particularly during periods outside of normal work hours, or when authorized personnel are not present to monitor security.
3. Access control systems must be maintained in good working order and records of maintenance, modification and repair activities should be available.
4. Wherever technically feasible, access logs that track incoming and outgoing activities should be reviewed on a periodic basis.
5. Systems located in public areas require special consideration. Every effort should be made to limit the amount of ePHI that is stored on such systems. Auto logoff, screen savers, proximity badge, and other device-specific hardware/software measures should be employed to maximally enhance security.
6. Maintenance records for physical security devices are maintained and available from UCDHS Plant Operations and Maintenance Division and the Information Services Division.

## STANDARD: Physical Security for the System

Physical Access Control measures are in place:

Building Level (Door Locks, Card Key, Controlled elevator access, etc.):

_____

Room Level (Door Locks, Card Key, etc.): _____

_____

Device Level (if any additional): _____

Physical Security Device maintenance records that are available in addition to UCDHS PO&M and UCDHS IS records (none additional required):

_____

_____

## SECTION 3: Backup Procedures

### Requirements

1. Backup copies of ePHI must be created and updated on a regular basis.
2. Frequency of backing up is dependent upon how frequently the information is modified, as well as the criticality of the data.
3. Backups may be performed to portable media (examples: CD-ROM, diskette, digital tape, etc.).
4. Alternatively, backup copies may be transferred to network file servers, if the data stored on the servers are backed up on a regular schedule and the archival media is stored in a safe, secure environment. For example, the network file servers maintained by UCDHS Information Services are completely acceptable for backup retention.
5. In the event of damage or malfunction of the system, backup media or alternative server data stores must be accessible within a reasonable period of time, in order to provide timely access to the ePHI for patient care or other immediate needs.
6. When portable media is discarded, it should either be overwritten or destroyed, eliminating all possibility that any ePHI contents could be read.
7. When a System is recycled, transferred to another user, or discarded, all storage devices or all ePHI records must be over written at least three times, rendering all ePHI records unreadable.
8. Backup Documentation – Backup maintenance should be documented.
9. Backup Log Review – For multi-user systems, the backup logs should be periodically reviewed by the appropriate supervisor or manager

## STANDARD: Backup Procedures

The following backup procedures will be maintained on the system.
Backups will be performed on:

### Option 1: UCDHS-IS (or equivalent) Network Server

Server Name: _____

Server Location (if not a UCDHS-IS server): _____

Drive and Directory Location of Copies: _____

### Option 2: Portable Media

Media Type (CD-ROM, diskette, etc.):_____
Media will be stored at the following location: _____

Backup Frequency:
Backups will be performed at least every: _____
Backup Documentation: Backup Maintenance will be documented by using:

1. The included Workbook Backup Log Sheets (see Appendix 2 for System Backup Log Sheets):_____
2. Equivalent Alternative:_____

## STANDARD: Manager/Supervisor Review

1. System administrators will use the included Multi-User System Backup Log Sheet that provides entries where supervisors can document their periodic review: _____
2. Equivalent Alternative: _____

## STANDARD: Media Destruction

All portable media (diskettes, CD-ROM's, etc.) will either be physically rendered unreadable, or all ePHI records will be overwritten at least three times prior to discard or reuse (Yes/No): _____

## STANDARD: System Recycling, Reuse or Discard

All storage devices on the system will either be:

1. Physically rendered unreadable
2. Overwritten at least three times.

(Yes/No):_____

## SECTION 4: Account Management and Access Review

### Requirements

1) Each User must be provided a unique account, with a unique User Name and Password.
2) Generic or shared accounts are not permitted.
3) Any written records of Account names and passwords should be kept in a locked, secure environment (not attached to a CRT for easy reference).
4) Access to a User's account must never be shared with another individual.
5) System administrators as well as individual users should maintain the recommended minimum practices for account and password maintenance. In the case where legacy systems cannot technically meet the minimum standards, passwords should reflect the maximum supportable length and complexity.
6) Passwords should be complex. Best practice is that they are composed of multiple character types, including: upper and lowercase alpha characters, numeric characters and symbols (#, $, etc.).
7) They should be at least 8 characters in length.
8) Authorization: For multi-user systems that are maintained by system administrators, there should be a formal system for authorizing user access. This may take the form of an account request form requiring management approval, or some electronic means of verifying that an account request is legitimate and authorized by the requesting department.
9) Account authorization as well as account management activities should be logged.
10) Management should review Account Logs on a periodic basis.

## STANDARD: Account Maintenance Logging

1. The included Multi-User System Account Maintenance Log will be used to document system account activities (see Appendix 2) (Yes/No): _____

   Equivalent Alternative: _____

   _____

## STANDARD: The following password standards will be maintained on the system

| Requirement | Standard |
|---|---|
| | |
| Minimum Length | |
| Upper and Lower Case Supported | |
| Symbols Supported | |
| Frequency of Password Change | |

## STANDARD: Generic Accounts not permitted

Any generic accounts have been removed (Yes/No): _____

## System Access Review

System administrators should periodically review the appropriate System Access Logs to ensure that there has not been attempted or actual unauthorized access to the system.

### Requirements

1) Administrators should familiarize themselves with the various system logs that record successful and unsuccessful login and logoff activity.
2) Logs should be reviewed on a periodic basis. A reasonable standard would be to review logs every two weeks.
3) Documentation of the periodic reviews should be maintained.
4) If suspicious activity is detected, contact the UCDHS Customer Support Center for further assistance and guidance.

## STANDARD: The following log file review standards will be maintained on the system

1. The System Log File(s) will be reviewed every _____days.
2. The Access Review Log Sheet will be used to document the reviews (see Appendix 2 for the System Access Review Log Sheet) (Yes/No): _____
   Equivalent Alternative: _____
   _____

## SECTION 5: Emergency Access

### Requirements

1) Users must ensure that in the event of emergency situations, the ePHI information on the System can be accessed when they are unavailable to provide access through normal means.
2) The procedure for emergency access should be reliable. For example, a system that relies upon the primary user to respond to pager or cell phone messages is not reliable, since there are a variety of likely scenarios wherein the primary user may not receive the message, or respond to it in a timely fashion.
3) The emergency access protocol should be written and should be communicated in advance to multiple individuals within the organization.
4) An acceptable protocol would be to: 1) create an account and password with all necessary access privileges; 2) place the information in a sealed, signed envelop; 3) place the envelope in a locked, secure location; 4) notify several responsible individuals within the immediate organization and provide them with the necessary means to access the envelope.

## STANDARD:

The following emergency access protocol has been established that provides for emergency access to the system during the absence of the primary user:

The following Individuals who are regularly available in the immediate work area have been informed and are prepared to execute the emergency access protocol:

## Section 6: Disaster Recovery

### Requirements

All systems that contain ePHI are susceptible to catastrophic damage or destruction by unforeseen environmental or other causes. Provisions must be made to ensure that ePHI records that are stored on the system are not irretrievably lost, should catastrophic damage or failures occur.

1. ePHI should be archived ("backed up") to portable media on a regular basis. Portable media can include: diskettes, network drives, CD-ROM, digital tape. See Section 3 "Backup Procedures", for further information on archival requirements.
2. Current copies of the archival media should be stored at a remote location that is unlikely to be affected by a local disaster. This media would be used to retrieve the ePHI, in the event that the system or local archival media are destroyed.
3. A "Disaster Recovery Plan" must be prepared that specifies the procedures to be implemented in order to resume access to ePHI following a disaster.
4. An acceptable Disaster Recovery Plan may consist of one or more of the following (or an equivalent plan developed by the system owner).

### Acceptable Disaster Recovery Plans

1. All ePHI on the system is archived on a regular basis onto a network server that is maintained by the UCDHS Information Services Division. IS has a comprehensive Disaster Recovery Plan. In the event of a disaster, UCDHS IS will provide for recovery of the ePHI.
2. Data is archived on a regular basis onto portable media and stored at a Remote Location. The format of the archival media is compatible with systems that are maintained in the UCDHS IS and for which comprehensive disaster recovery facilities are available. In the event of a disaster, remotely stored copies of the media will be retrieved and UCDHS IS will assist in recovery the ePHI records.
3. Copies of media are remotely stored as in option 2. A system located remotely (not maintained by UCDHS-IS) is available that will be used to recover the ePHI.

**STANDARD: The following Disaster Recovery Plan will be implemented in the event of catastrophic loss of the primary system.**

### Option 1

1. ePHI will be archived to a network file server that is maintained by UCDHS-IS.

2. The name of the server and the directory location of the data are as follows: _____

3. ePHI data will be archived to the network server every (day, week, etc.) _____

4. In the event of a disaster, UCDHS-IS Customer Service will be contacted, who will arrange for recovery and access to the ePHI.

### Option 2

1. ePHI will be archived to portable media on a regular basis; at least once every _____

2. Archival media type and format are as follows (example: CD-ROM, Windows 2000 format): _____

3. Archival media will be labeled as follows:

4. Copies of the archival media will be stored at the following remote location (give specific location information): _____.

### Option 3

1. In the event of catastrophic loss of the primary system, an alternative system will be used to recover the ePHI. The alternate system(s) is located at: _____

Equivalent Alternative Plan: _____

_____

### Disaster Plan Notification

The following individuals have been informed of this Disaster Recovery Plan and are prepared to execute it (Name, Title, Contact Information).

1. _____

2. _____

## SECTION 7: Email Security

### Requirements

1. UCDHS Email Policy specifies that email communications that contain ePHI must use an approved UCDHS email system or service. No restrictions apply to any email messages that do not contain ePHI.
2. For email communications internal to UCDHS, both sender and receiver must use the UCDHS Lotus Notes Email System.
3. If Relay Health is available, email communications between clinicians and patients must use that service. Clinicians can also use the Relay Health Email Service to communicate securely with outside clinicians and researchers. This is a good interim solution for secure email transmission, pending completion of a UCDHS encrypted email service, currently under development.
4. Email communications to outside email systems that contain ePHI are strongly discouraged unless the message is encrypted. Outside email systems include the UC Davis Email System.
5. UCDHS IS is developing a method of encrypting outgoing email messages within the Lotus Notes Email System, using a widely supported protocol called S/MIME. The system will support secure transmission of messages to external email systems that support the S/MIME standard. The new system is projected to be available my mid-2005. In the interim, files may be encrypted using a suitable software program such as WinZip.
6. Further information regarding the UCDHS-approved email systems may be obtained by contacting the UCDHS Information Services Customer Support Center.

## STANDARD: Email Security Procedures

Email is sent/received on the system (yes/no) _____

If email is sent/received on the system, usage adheres to UCDHS Requirements 7.1 listed above (yes/no) _____

Until a UCDHS Secure Email Service is available, I will defer from emailing ePHI. Otherwise, the following email encryption methodology will be used:

_____

_____

Equivalent Alternative: _____

_____

Or, if encryption will not be used, reason: _____

_____

## SECTION 8: System Security Management Practices

### Requirement

1. Systems should be kept current with software upgrades (patches) that correct security deficiencies or enhance the capability to prevent unauthorized access.
2. Software patches are generally provided to licensed customers free of charge by software vendors. Users should subscribe to all available software upgrade services and install new security patches as they become available. Information regarding the availability of security and other software patches for Microsoft software may be found at the Microsoft Corporation Web site: Microsoft.com.
3. Systems should have Virus Protection Software installed.
4. The Virus (or Worm) Protection Software should be regularly updated by downloading the latest virus information files; in order to protect the System from infection by newly identified viruses.
5. System operating system software should be configured to "auto-logoff" after a brief period of inactivity. This will reduce the possibility that an unauthorized party can access an unattended system.

6. UCDHS Information Services Customer Support Center (IS-CSC) will soon make available the McAfee Virus Protection Software System. This software will be provided free to any UCDHS faculty, staff, or student. The software will be made available at the following Web address: intranet.ucdmc.ucdavis.edu/iscss.html. The Web site should be operational by the middle of May 2005.
7. UCDHS IS-CSC will soon make available the Altiris Software delivery agent. By installing the Altiris software agent on their PC's users will have all UCDHS – recommended security and other patches for Microsoft Operating Systems. Other software automatically "pushed" to their PC and remotely installed, eliminating the need for any manual maintenance by the system owner. This software will be provided free to any UCDHS faculty, staff, or student. The software will be made available at the following Web address: intranet.ucdmc.ucdavis.edu/iscss.html. The Web site should be operational by the middle of May 2005.

## STANDARD – System Patches

Systems will be regularly upgraded with current security patches by using the following update procedure:

1. Option 1: The Altiris software delivery agent, provided by the UCDHS IS-CSC, will be installed on the system. This software will automatically update the system with needed patches. _____
2. Option 2: Patches will be obtained from the software vendor and installed on a regular basis. _____

## STANDARD – Virus Protection Software

One or more of the following procedures will be used to keep current with the latest Virus Information Files available for the Virus Protection Software:

1. I subscribe to the following non-UCDHS virus software update service. _____
2. I will regularly download Virus Information Files from the Application Vendor: _____
3. I plan to subscribe to the UCDHS IS-CSC Virus Protection Service, which should be available by mid-May 2005. _____
4. Equivalent Alternative: _____

## STANDARD – Auto Logoff

1. The Systems have been configured to Auto-Logoff after the following period of inactivity: _____
2. Alternative: The system has been configured for a password-protected screensaver after the following period of inactivity: _____
3. Alternative: The system is incapable of options 1 or 2: _____

## Appendix 1 - Contact Information and HIPAA Regulations References

UCDHS Information Services Customer Support Center
Phone: 916-734-4357

UCDHS HIPAA Security Office:
Phone: 916-703-6591
Email: Hipaa.security@ucdmc.ucdavis.edu

UCDHS HIPAA Compliance Office
Phone: 916-734-8808
Email : rory.jaffee@ucdmc.ucdavis.edu

HIPAA Regulations References:
http://compliance.ucdmc.ucdavis.edu/guidance/privacy/security/rule.html

HHS Web Site:
http://aspe.hhs.gov/admnsimp/index.shtml

UCDHS HIPAA Security Web Site:
http://compliance.ucdmc.ucdavis.edu/guidance/privacy/security/

UCDHS HIPAA-related Policies:
http://compliance.ucdmc.ucdavis.edu/guidance/privacy/

For more information:

- Full text of HIPAA regulations as of April 17, 2003.
- HIPAA administrative simplification act
- Privacy case examples
- Office for Civil Rights — Privacy of Health Records
- Am I a covered entity? A decision tool developed by DHHS
- Internet Use Guidelines from the Federation of State Medical Boards
- The right to privacy - The seminal law article in the United States. Discusses threat to privacy by new technologies. Written in 1890.
- Penalties under HIPAA
- California Privacy Laws

## Appendix 2 – System Log Sheets

1. Backup Log Sheet
2. System Access Review Log
3. System Account Maintenance Log

## MULTI-USER SYSTEM BACKUP LOG SHEET

Use this Log Sheet to document regular backup procedures. Separate Log Sheets should be maintained for each System covered by this Workbook.

### System Identification

Description:

_____

Serial or Property Number:

_____

Location:

_____

### Activity Log

| Date | Operator | Incremental Back-Up Date | Full Back-Up Date | Offsite Copy Update |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Manager/Supervisor Review and Comments

| Date | Manager Identification | Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## System Access Review Log

Use this log sheet to document the periodic review of Computer Access Logs

## System Identification

Description:

_____

Serial or Property Number:

_____

Location:

_____

| Date | Reviewer | Findings |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## Multi-User System Account Maintenance Log

Use this log sheet to document the following Account activities:

- Authorization
- Creation
- Deletion
- Inactivation
- Password Change

## System Identification

Description:

_____

Serial or Property Number:

_____

Location:

_____

| Date | Person | Authorization | Account Name | Function (Create/Delete/ Password Change) | Performed By |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

For multi-user systems maintained by a system administrator, the supervisor or manager should periodically review the Account Management logs

## Manager/Supervisor Review and Comments

| Date | Manager Identification | Comments |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |