

## 1.0 Purpose

The purpose of these procedures is to outline methods of securing UCSF computing resources from unauthorized access.

The HIPAA Security Standard and Implementation Specifications that govern this procedure are:

*164.312(a)(1) Access Control (Required).* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).

*164.312(a)(2)(i) Unique User Identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

*164.312(a)(2)(ii) Emergency Access Procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

*164.312(a)(2)(iii) Automatic Logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

*164.312(a)(2)(iv) Encryption and Decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

## 2.0 Definitions

**2.1 Identification:** Identification is the means by which a user provides a claimed identity to the system.

**2.2 Workforce:** All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

## 3.0 Procedures

**3.1 Unique User Identification:** System managers and owners are responsible for requiring assignment of a unique user ID for all users of systems that access restricted or confidential information.

**3.1.1 Use of unique user identification:** Users of systems that access restricted or confidential information are required to identify themselves utilizing their own unique user ID.

**3.1.2 Correlate actions to users:** As technically feasible, systems used to access restricted or confidential information should internally maintain the identity of all active users and link system actions to specific users.

**3.1.3 Maintenance of user identification:** Timely user identification maintenance is required for all user IDs on systems used to access restricted or confidential information. Maintain a current record of unique user IDs through the process of deleting inactive or terminated user IDs, modified or transferred job duties and adding new ones.

**3.1.4 Disabling inactive user IDs:** System managers and owners are responsible for disabling user IDs that have remained inactive for a specific period of time (such as 90 days).

**3.1.5 No sharing of user IDs:** If users share ID's, it makes it impossible to prove who actually accesses an application. Therefore, all users are responsible to not share their user IDs that allows access to restricted or confidential information with anyone.

**3.2 Emergency Access Procedures:** System managers and owners are responsible for implementing procedures when providing access to restricted or confidential information in the event of an emergency. Test access, authorization and auditing to ensure compliance remains constant with that of normal operations.

**3.2.1 Authorize emergency access:** Directions containing criteria for authorization and listing user names should be established for authorizing access to restricted or confidential information based upon the business needs and job function of the individual who requires emergency access.

**3.2.2 Establish emergency access rights:** Directions containing criteria for granting access rights should be established for access to restricted or confidential information. This includes access to the physical environment and to the contingency systems where emergency access is provided. Criteria should include answering the following:

- Who are you?
- Why do you require access?
- Can you prove you are who you claim to be?

**3.2.3 Log details of emergency access:** User access should be

---

If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

audited and monitored during emergency access to restricted or confidential information. Logs to be maintained capturing the details of the emergency access should include:

- Date and time the access was granted
- Individual name and contact information requiring access
- Individual unique user ID
- Access rights provided (system, data)
- Nature of the emergency
- Authorizers name

**3.3 Automatic Logoff Procedures:** System managers and owners are responsible for implementing procedures specific to systematic termination of user's electronic session due to non-activity. Automatic logoff is required to make sure that unauthorized users do not recycle existing sessions if a user leaves a workstation.

**3.3.1 Establish allowable non-activity duration:**

Based upon the type of activities the users perform while accessing restricted or confidential information, system managers and owners are responsible for establishing a reasonable duration of non-activity that ensures the security of restricted and confidential information is not compromised.

**3.3.2 Restrict administration of automatic logoff:**

System managers and owners are responsible for restricting access to automatic logoff parameters to authorized personnel only.

**3.3.3 Require user re-establishing electronic sessions:**

System managers and owners are responsible for requiring that users re-identify themselves uniquely before being allowed to perform any actions on the system, when logged off of an electronic session due to non-activity.

**3.4 Encryption and Decryption Procedures:** Implement procedures when the process of encrypting and decrypting data is deemed necessary. Encryption technologies may be used to make sure that confidential information are not accessible by entities that are not authorized to use it.

**3.4.1 Select encryption and decryption methods:**

System managers and owners are responsible for selecting the encryption and decryption methods

appropriate to their technical environment. When selecting the encryption and decryption method to be deployed, utilize only standards accepted by an industry standards governing body such as ANSI, ISO and NIST.

**3.4.2 Define standards for when data must be encrypted:** System managers and owners are responsible for defining the specific conditions concerning when data must be encrypted, taking into consideration the potential risk of storing or transmitting the data unencrypted.

**3.4.3 Define key management procedures:** System managers and owners are responsible for defining the methods for managing and communicating public and/or private keys for encrypting and decrypting data.. Key management methods must be in accordance with UC policy.

#### **4.0 Initiation and Control Reporting**

---

#### **5.0 Records & Documentation Control**

---

### 6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Audit Controls	<b>164.312(b)</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Special Publication: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule – National Institute of Standards and Technology (NIST)	<b>SP 800-66</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
University of California Business and Finance Bulletin IS-3 Electronic Information Security	<b>BFB IS-3</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a> or <a href="http://www.ucop.edu/ucophome/policies/bfb/is3.pdf">http://www.ucop.edu/ucophome/policies/bfb/is3.pdf</a>
Information Security and Confidentiality Policy (UCSF Campus)	<b>650-16</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Information Security and Confidentiality Policy (UCSF Medical Center)	<b>5.01.04</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>
Security Management Procedures Information Access Management Procedures	<b>60.001</b> <b>60.003</b> <a href="http://www.ucsf.edu/hipaa/dpt_compliance/">http://www.ucsf.edu/hipaa/dpt_compliance/</a>

### REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	01/28/05	Ellen Amsel, Binh Nguyen and Dan Yee	Initial Release
B	03/18/05	Dan Yee and Barbara Heredia	Version 1.2, section 3.0 Procedures
C	01/02/2007	Rob Slaughter	Adapted for School of Nursing

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.  
 Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 01/02/2007