

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

System Access Control Procedures

Revision B

Dean's Office
Information Services Unit
Issue Date: 5/12/05
Last Revision: 3/21/05

identify themselves utilizing their own unique user ID.

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

3.1.2.1 ISU developed applications will correlate actions to users. It is not technically feasible for actions to be correlated to users on ISU file servers.

3.1.3 Maintenance of user identification: Managers are required to submit account activation and account termination forms to ISU on a timely basis.

3.1.4 Disabling inactive user IDs: The SOM Strong Password policy has a password expiration of 90 days. All accounts with passwords older than 90 days cannot be accessed until the user calls the ISU Help Desk (415-502-1919).

3.1.5 No sharing of user IDs: It is the responsibility of every user to keep their login credentials private. Users cannot share 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.

3.2.1 Authorize emergency access: Managers must provide the ISU Helpdesk with an [Access to Sensitive Data Form](#) for emergency access to data. Managers must fax the completed form to the ISU Helpdesk (415-502-2255).

3.2.2 Log details of emergency access: The ISU Help Desk will log request details in the Remedy system. The original form will be kept on file.

3.3 Automatic Logoff Procedures: All systems that access ePHI will be required to have a password protected screensaver enabled with inactivity duration of 10 minutes. Automatic logoff is required to make sure that unauthorized users do not recycle existing sessions if a user leaves a workstation.

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 ISU Encryption Requirements for stored ePHI

3.4.2.1 Server Files – Primary Disk Storage

No encryption methodologies will be employed on ISU file servers because they have sufficient security and shared encryption/decryption is technically too difficult to institute.

3.4.2.2 Tape Backup

ISU will secure all tape backups with a complex password. No encryption methodologies will be employed due to the low risk of data being loss.

3.4.2.3 Workstations including desktops, laptops, and Blackberry PDAs.

ISU will offer campus supplied Pretty Good Privacy (PGP) solution for users who require ePHI to be stored on workstations and laptops.

Encryption on Blackberry's is pending a Blackberry server software upgrade, expected in FY '05-06.

3.4.2.4 SQL Server Databases

Databases are not encrypted but research is underway to encrypt ePHI databases using SQL Server technology.

3.4.3 ISU Encryption Requirements for transmitted ePHI

3.4.3.1 ISU's Personnel Database (PDB) which transmits sensitive personnel data (though

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.

System Access Control Procedures

Revision B

Dean's Office
Information Services Unit
Issue Date: 5/12/05
Last Revision: 3/21/05

no SSN or ePHI) between database and client is a COM+ application which takes advantage of Windows Server 2000's native encryption and authentication technologies including RSA Security's RC4 encryption algorithm with 128-bit keys and Kerberos authentication.

3.4.3.2 External and Internal File Transfers/Remote Access

ISU employs IPSEC, VPN, and/or Secure FTP

3.4.3.3 Information on the Internet

ISU employs Secure Sockets Layer (SSL), which uses a public key infrastructure (PKI) to encrypt data in transmission using 256-bit encryption.

3.4.4 Define key management procedures: Data owners must keep encryption keys secure and separate from the data being encrypted. Key management methods must be in accordance with UC policy.

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

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 03/29/2005

System Access Control Procedures

Revision B

Dean's Office
Information Services Unit
Issue Date: 5/12/05
Last Revision: 3/21/05

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Audit Controls	164.312(b) http://www.ucsf.edu/hipaa/dept_compliance/
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)	SP 800-66 http://www.ucsf.edu/hipaa/dept_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	BFB IS-3 http://www.ucsf.edu/hipaa/dept_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
Information Security and Confidentiality Policy (UCSF Campus)	650-16 http://www.ucsf.edu/hipaa/dept_compliance/
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dept_compliance/
Security Management Procedures Information Access Management Procedures	60.001 60.003 http://www.ucsf.edu/hipaa/dept_compliance/

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	04/11/05	Todd Lawrence	Converted to S/Med Template

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 03/29/2005