

1.0 Purpose

1.1 Security Awareness and Training: The purpose of this document is to outline the training plan and scope of the awareness and training program as required by the HIPAA Security Standard: *164.308(a)(5)(i) Security Awareness and Training*: Implement a security awareness and training program for all members of the UCSF workforce (including management). The HIPAA Privacy Rule training and education model will be utilized for security training as well. Awareness and training procedures in this document include:

- **Initial Workforce Training Strategies:** Implement procedures for the initial training of the UCSF workforce prior to April 21, 2005 as well as for all new employees after April 21, 2005.
- **On-going security awareness and training:** Implement procedures to ensure employees receive security training and procedures for periodic security updates.

1.2 164.308(a)(5)(ii)(B) Protection from Malicious Software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

1.3 164.308(a)(5)(ii)(C) Log-in Monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

2.0 Definitions

2.1 Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2.2 Availability: The property that data or information is accessible and usable upon demand by an authorized.

2.3 Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

- 2.4 Health Care Providers:** Any provider of medical or other health services, or supplies, that transmits any health information in electronic form in connection with a transaction for which a standard has been adopted.
- 2.5 Individual:** The person who is the subject of protected health information.
- 2.6 Integrity:** The property that data or information has not been altered or destroyed in an unauthorized manner.
- 2.7 Protected Health Information (PHI):** PHI is an individual's health information or data collected from an individual that is created or received or received by a health care provider, plan or clearinghouse related to the past, present or future physical or mental health condition of an individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual; identifies or could reasonably identify the individual; and is transmitted or maintained in electronic or any other form or medium. Note: This excludes the individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) of the Social Security Act, and employment records held by a covered entity in its role as employer.
- 2.8 Security or Security measures:** Encompasses the entire administrative, physical, and technical safeguard in an information system.
- 2.9 Use:** With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.
- 2.10 User:** A person or entity with authorized

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.

access.

- 2.11 **Workforce:** All faculty, staff, students, trainees, volunteers, and business associate who access restricted or confidential information during the course of their duties.
- 2.12 **Workstation:** An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment.

2. Procedures & Responsibilities

3.1 Workforce Security and Awareness Training for all Members of the UCSF Workforce

- 3.1.1 Security training tools will be developed by the Information Security Officer, in consultation with the HIPAA HR and Education committee, before April 20, 2005, and provided to the Departments in a timely manner so that training can occur. Training tools may include: HIPAA Security Awareness Training (HIPAA Security 101); training materials to be mailed to all employees; on-line training materials, including power point presentations, specialized training sessions as needed for employees responsible for implementing specific physical or technical safeguard; and the HIPAA Handbook.
- 3.1.2 This training will be provided to each member of the workforce by no later than April 19, 2005. Each Department is responsible for determining and implementing appropriate and reasonable training methods that are most appropriate for meeting the training needs of the Department's workforce. Training methods may include, but are not limited to: departmental meetings or training sessions; on-line training sessions; or attendance at large-group training

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.

sessions offered to workforce members enterprise-wide; or mass mailing of a Security Awareness brochure combined with one or more of the above training methods.

- 3.1.3** Department will document that the workforce has completed HIPAA Security Awareness Training

3.2 On-going Security Awareness and Training and Security Updates

- 3.2.1** Security and training awareness will be incorporated into new employee orientation process by April 21, 2005.
- 3.2.2** Departments will conduct staff training whenever they are notified of significant changes to procedures and policies.
- 3.2.3** The Information Security Officer and/or the Privacy Officer will keep the following apprised of Security Training activities:
- Core HIPAA Committee
 - HIPAA Steering Committee
 - Executive Medical Board
 - General Advisory Council
 - Executive Management for the UCSF Enterprise.
 - The Office of the President and the Board of Regents as may be required for annual compliance reporting to the University's governing body.
 - IT Governance Committee

3.3 Protection from Malicious Software: Anti-virus software must be installed and kept up-to-date either through a UC provided solution or directly from the anti-virus manufacturer.

3.4 Log-in Monitoring: Domain login attempts will be monitored through the Windows security event

log. Suspicious login activity such as multiple login attempts from unknown domains, accounts and machines within a short duration of time will be reviewed weekly. Any suspicious activity will be reported to IT Security. Logs containing any suspicious activity will be saved as csv files in a protected location only accessible by SOM domain administrators. Logs will be burned to CD (or DVD, dependent upon size) on an annual basis and sent offsite. Retention time for media will be six years.

4.0 Initiation and Control

Reporting

5.0 Records & Documentation Control Departments will maintain their records of security training for staff as documentation of compliance.

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rule: Security Awareness and Training	164.308(a)(5) 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/ucophome/policies/bfb/is3.pdf
UCSF Information Security and Confidentiality Policy	650-XX http://www.ucsf.edu/hipaa/dept_compliance/
UCSF Medical Center Administrative Policy - Information Security and Confidentiality Policy	5.01.04 http://www.ucsf.edu/hipaa/dept_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	01/07/05	Carl Tianen and Deborah Yano-Fong	Initial Release
B	2/24/05	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.