

Owner: Darlena Torres, Manager, IT Customer Support Center	Date Approved:
Authorized By: Jose Claudio, Director, IT Infrastructure & Security	Date Approved:

## 1.0 Purpose

- 1.1. Implement policies and procedures to ensure that all members of the UCSF Medical Center workforce have appropriate access to electronic protected health information, and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.
- 1.2. Workforce Security Procedures establish standards for implementing:
  - 1.2.1. Authorization and/or Supervision Procedures
    - Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
  - 1.2.2. Workforce Clearance Procedures
    - Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
  - 1.2.3. Termination Procedures
    - Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in the Workforce Clearance Procedures.

## 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. **Access-Granting Group:** The group responsible for administering access rights to users.
- 2.3. **Availability:** The property that data or information is accessible and usable upon demand by an authorized.
- 2.4. **Confidentiality:** The property that data or information is not made available or disclosed to unauthorized persons or processes.
- 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:** Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium. 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. **Sensitive Information:** This includes Electronic Protected Health Information (ePHI) as well as other private personal information such as payroll records and other confidential files.
- 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 access.
- 2.11. **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 & Responsibilities

#### 3.1. Authorization and/or Supervision Procedures

- 3.1.1. Define roles and responsibilities for all job functions.
- Roles and responsibilities are defined, documented, and authorized in the job descriptions generated in each department.
  - Job descriptions are then sent to, authorized by, and centrally stored in the Human Resources (HR) department.
- 3.1.2. Identify in writing who has the business need – and who has been granted permission – to view, alter, retrieve, and store electronic health information, and at what times, under what circumstances, and for what purpose.
- Department Managers are responsible for identifying which of their direct reports, or users, require access to sensitive information.
  - The Department Manager must then identify the systems their direct reports require access to in their daily work that contain access to sensitive information. The

appropriate Logon ID Request Forms (located at: <http://it.ucsfmedicalcenter.org/>) must be filled out and sent to the access-granting group for processing.

Both the department manager and the user must sign these forms prior to processing by the access-granting group.

- The department must keep a copy of the Logon ID request. These forms are also centrally stored with the access-granting group.
- Department Managers are responsible for terminating access for their direct reports who are transferred to another department or employment ends as defined in section 3.3 Termination Procedures.

### 3.2. Workforce Clearance Procedures

3.2.1. Ensure that staff members, in positions involving access to and use of sensitive information, have the necessary knowledge, skills, and abilities to fulfill particular roles.

- Department Managers are responsible for maintaining authorization records for the direct reports with access to systems with granted access to sensitive information as identified in section 3.1. Authorization and/or Supervision Procedures.
- Department Managers are responsible for making sure their staff is trained on the systems granting access to sensitive information as well as maintaining training records for each staff member.

3.2.2. Ensure that the requirements as stated in section 3.2.1 are included as part of the personnel hiring process.

- All employees submit to a criminal background check, social security trace for all positions prior to employment. Employees responsible for sensitive information and cash handling also get fingerprinted. These records are kept in Human Resources.
- Upon hire and regardless of position or system access, all UCSF employees must sign the University of California San Francisco Confidentiality of Patient, Employee and University Business Information Form (located at: <http://hr.ucsfmedicalcenter.org/forms.HTM>)
- This signed form is stored in Human Resources.

### 3.3. Termination Procedures

- 3.3.1. Ensure access to electronic protected health information is terminated when the employment of a workforce member or user ends or changes.
- The Department Manager is responsible for completing the Personnel Action Form (located at <http://hr.ucsfmedicalcenter.org/forms.HTM> ) and sending it to HR for processing.
  - HR will process the termination in the Human Resources database.
  - HR will notify the appropriate access granting groups for account termination.
  - The access-granting group will record the deactivation of user access accounts.

**4.0 Initiation and Control Reporting**

- **Completed Records Stored with the appropriate access-granting group:** Logon ID Request Forms, Termination Notification List, and Account Deactivation Records.
- **Completed Records Stored in HR:** Job Description and University of California San Francisco Confidentiality of Patient, Employee and University Business Information Form.
- **Completed Records Stored in Requestor Department:** Logon ID Request Forms, University of California San Francisco Confidentiality of Patient, Employee and University Business Information Form, and Training Records.

**5.0 Records**

- Job Description
- Logon ID Request Forms
- University of California San Francisco Confidentiality of Patient, Employee and University Business Information Form
- Training Records
- Personnel Action Form
- Termination Notification List
- Account Deactivation Records

Per 164.316 Policies and Procedures: Documentation Requirements, Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

**6.0 Related Records**    **164.308(a)(3) - HIPAA Security Rule: Workforce Security**

**REVISION RECORD**

Rev.	Date	Originated by:	Description of Change
A	11/17/2004	Darin Reinwald	Initial Release

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.