

1.0 Purpose

Implement policies and procedures to ensure that all members of the Department of Family & Community Medicine workforce have appropriate access to protected health and sensitive information, and to prevent those workforce members who do not have access from obtaining access to protected health and sensitive information.

1.1. Workforce Security Procedures establish standards for implementing:

1.1.1. Authorization and/or Supervision Procedures

- Implement procedures for the authorization and/or supervision of workforce members who work with protected health and sensitive information or in locations where it might be accessed.

1.1.2. Workforce Clearance Procedures

- Implement procedures to determine that the access of a workforce member to protected health and sensitive information is appropriate.

1.1.3. Termination Procedures

- Implement procedures for terminating access to electronic protected health and sensitive information when the employment of a workforce member changes or ends.

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 employee Job Descriptions.
 - Job Descriptions are authorized by and centrally stored in the Department Personnel Office and Campus Human Resources (HR).
 - Significant changes in duties need to be documented in a revised Job Description.
- 3.1.2. Identify in writing who has the business need – and who has been granted permission to access/use (to view, alter, retrieve, and store) protected health and sensitive information and at what times, under what circumstances, and for what purpose.
 - Department Manager/Unit Managers/Unit Directors are responsible for identifying which of their employees require access to protected health and sensitive information.
 - Department Manager/Unit Managers/Unit Directors must identify the information systems their employees need access to and initiate procedures to authorize and obtain

access privileges.

- Information systems that contain protected health and sensitive information may include computer service such as networked shared drives/desktops/laptops requiring basic computer access/Logon/password and/or systems that require a separate Logon ID (i.e., Campus ITS OLPPS and Weblinks, Medical Center and CHN patient information systems).
- Appropriate Logon ID Request or Account Creation and Account Termination Forms (for access initiation, modification and termination) must be completed and sent to the access-granting group for processing.
- Forms such as the School of Medicine's Request for Access to Sensitive Information must be completed if required by the access-granting group (http://intranet.medschool.ucsf.edu/info_tech/pdf/Request_Access_Sensitive_Data.pdf).
- If Department Manager/Unit Managers/Unit Directors require the transfer of access permissions from one user/employee to another, the UCSF Tracking Form for Access With or Without Consent to Electronic Communications Records Form must be completed and sent to the access-granting group for processing (<http://www.ucsf.edu/its/policy/tracking-form.pdf>).
- Each unit must keep a copy of all access and consent request forms. These forms are also centrally stored with the access-granting group.
- Department Manager/Unit Managers/Unit Directors are responsible for terminating employee systems access if job responsibilities are modified, upon transfer to another department or when UCSF employment ends (as defined in Section 3.3 Termination Procedures).

3.2. Workforce Clearance Procedures

- 3.2.1. Ensure that employees, in positions with access to and use of protected health and sensitive information, have the necessary knowledge, skills, and abilities to fulfill particular roles.
 - Department Manager/Unit Managers/Unit Directors are responsible for maintaining authorization records for employees who have authorized access to systems and

protected health and sensitive information as identified in section 3.1. Authorization and/or Supervision Procedures.

- Department Manager/Unit Managers/Unit Directors are responsible for making sure authorized employees are trained on systems with protected health and sensitive information as well as maintaining training records for each employee.
- 3.2.2. Ensure that the requirements as stated in section 3.2.1 are included as part of the personnel hiring process.
- 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://www.ucsfhr.ucsf.edu/staffing/files/HIPAAConfidentialityStatement.pdf>)
 - This signed form is stored in the employee's personnel file in the Department Personnel Office.

3.3. Termination Procedures

- 3.3.1. Ensure access to electronic protected health and sensitive information is terminated when an employee transfers to another department, when UCSF employment ends or when job responsibilities are modified.
- The Department Manager/Unit Managers/Unit Directors are responsible for notifying the Department Personnel Office of an upcoming separation or transfer.
 - The Department Personnel Office will process the termination in the Human Resources database.
 - The Department Manager/Unit Managers/Unit Directors will submit the required forms for user account termination to the access-granting group. The School of Medicine Access Termination Form can be found at: http://intranet.medschool.ucsf.edu/info_tech/policies/security/HIPAA.aspx.
 - 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 Form or Access Creation Form, Access Termination Form, Request for Access to Sensitive Information Form, UCSF Tracking Form for Access With or Without Consent to Electronic Communications Records and Account Deactivation Records.
- **Completed Records Stored in Employee Personnel File in Department Personnel Office:** Job Description and UCSF Confidentiality of Patient, Employee and University Business Information Form.
- **Completed Records Stored in Department Unit:** Logon ID Request Form or Access Creation Form, Access Termination Form, Request for Access to Sensitive Information Form, UCSF Tracking Form for Access With or Without Consent to Electronic Communications Records, UCSF Confidentiality of Patient, Employee and University Business Information Form and Training Records.

5.0 Records

- Job Description
- Logon ID Request or Account Creation Form
- Account Termination Form
- Request for Access to Sensitive Information Form
- UCSF Tracking Form for Access With or Without Consent to Electronic Communications Records
- UCSF Confidentiality of Patient, Employee and University Business Information Form
- Training Records
- Request for Payroll Action (as referenced in Section 3.3.1 Termination Procedures)
- 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