

1.0 Purpose

- 1.1. Implement policies and procedures for authorizing access to electronic protected health information as appropriate based upon business needs and job functions, as referenced in the UCSF 650-16 Information Security and Confidentiality Policy.
- 1.2. Information Access Management procedures in this document include:
 - 1.2.1. Information Access Authorization
 - Implement policies and procedures for granting access to electronic protected health information, for example, through access to a process, or other mechanism.
 - 1.2.2. Information Access Establishment and Modification
 - Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

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. **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.
- 2.6. **Individual:** The person who is the subject of protected health information.
- 2.7. **Integrity:** The property that data or information has not been altered or destroyed in an unauthorized manner.
- 2.8. **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.

- 2.9. **Sensitive Information:** This includes Electronic Protected Health Information (ePHI) as well as other private personal information such as payroll records and other confidential files.
- 2.10. **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.
- 2.11. **User:** A person or entity with authorized access.
- 2.12. **Workforce:** All faculty, staff, students, trainees, volunteers, and business associate who access restricted or confidential information during the course of their duties.
- 2.13. **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.

3.0 Procedures & Responsibilities

3.1. Criteria for Establishing Access

3.1.1. Granting Access:

- Department Manager/Unit Managers/Unit Directors are responsible for authorizing access to systems with sensitive information. Access rights will be granted as identified in the Workforce Security Procedure, section 3.1. Authorization and/or Supervision Procedures.

3.1.2. Restricting Access

- Access to sensitive information is restricted until granted as defined in section 3.1.1 Granting Access.

3.1.3. Identity Based Access

- Each user requires a unique User ID in order to gain access to sensitive information.

3.2. Information Access Establishment and Modification

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.

3.2.1. Establishing and Documenting Access Authorization

- As defined in the Workforce Security Procedure, section 3.1. Authorization and/or Supervision Procedures, Department Manager/Unit Managers/Unit Directors are responsible for identifying employees with responsibilities that 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. School of Medicine Forms can be found at:
http://intranet.medschool.ucsf.edu/info_tech/policies/security/HIPAA.aspx
- Forms such as the School of Medicine's Request for Access to Sensitive Information must be completed as 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 Workforce Security Procedures Section 3.3 Termination Procedures).

3.2.2. **Maintenance of access rights:**

- If changes are required to access permissions, follow the same procedures described in Section 3.2.1 Establishing and Documenting Access Authorization.

4.0 Initiation and Control Reporting

Completed records associated with this procedure are stored with the access-granting group & in department requesting authorization.

5.0 Records

- Logon ID Request or Account Creation and Account Termination Forms
- Request for Access to Sensitive Information Form
- UCSF Tracking Form for Access With or Without Consent to Electronic Communications Records Form

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)(4) - HIPAA Security Rule: Information Access Management
60.002 – Workforce Security Procedure

REVISION RECORD

Rev.	Date	Originated by:	Description of Change

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.