

# Physical Safeguards: Workstation Use Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 04/11/05

---

## 1.0 Purpose

The purpose of this document is to define procedures to meet the following HIPAA Security Physical Safeguards Standard:

*164.310(b) Workstation Use.* Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation that can access electronic protected health information, to restrict access to authorized users.

## 2.0 Definitions

- 2.1 Business Associate (BA):** A person or entity that has access to protected health information (PHI) as a result of providing services to or for a covered entity. A BA performs a function or activity on behalf of UCSF Medical Center involving the use or disclosure of PHI such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing.
- 2.2 Mobile Computing Device:** A mobile-computing device is a laptop or tablet PC, PDA, or any other device that performs similar functions, along with storage media and peripherals connected to the device.
- 2.3 Workforce:** All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.
- 2.4 Workstation:** An electronic computing device, including laptop, tablet PC, desktop computer, PDA, or any other device that performs similar functions, as well as the electronic media stored in its immediate environment such as local hard drives, CDROMs, floppy drives, zip-drives that are directly connected to the device.

## 3.0 Procedures

### 3.1 Acceptable Workstation Use

#### 3.1.1 Department and Unit Managers must:

- 3.1.1.1** Inventory workstations and devices.
- 3.1.1.2** Define what functions for a workstation or class of workstations is proper; functions include general network access, department intranets, email access, Internet access, mapped network drives, applications that run on the

---

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 02/22/05

---

## Physical Safeguards: Workstation Use Procedures

Revision B  
*Dean's Office*  
Information Services Unit  
Issue Date:  
Last Revision: 04/11/05

---

workstation, allowable activities for each workstation.

### 3.1.2 Workforce and Business Associates must:

- 3.1.2.1 Obtain approval from department or unit manager before accessing workstations, systems or applications.
- 3.1.2.2 Exercise care in protecting the workstations from access by unauthorized persons; and for safeguarding sensitive information from being accessed, viewed or erased by unauthorized persons.
- 3.1.2.3 Users are required to log off of applications containing patient health or sensitive business information *before* leaving their workstations.
- 3.1.2.4 Network file server shared drives should be used to store sensitive or critical files.
- 3.1.2.5 Workstations are required to have an enabled password-protected screensaver set to engage after 10 minutes of inactivity. In cases where password-protected screen savers are not available, non-password-protected screen savers should be enabled.
- 3.1.2.6 The S/Med ISU has established standard configurations for desktop technologies. Computers, computer peripherals and software should meet the standard.
- 3.1.2.7 Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs (Graphic Interface Files), by employees is prohibited. Software required for end user purposes must be approved and installed by ISU. The end user must document and maintain proof of license to have such applications. Software installations will be coordinated through the ISU Help Desk.

### 3.2 Workstation Physical Safeguards

---

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 02/22/05

---

## Physical Safeguards: Workstation Use Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 04/11/05

---

- 3.2.1** Workstations that access PHI must implement the following measures:
- 3.2.1.1** Workstation monitors must be situated in a manner that prohibits unauthorized viewing.
  - 3.2.1.2** Desktops in open, common areas should be physically secured to prevent theft.
  - 3.2.1.3** Laptops and mobile computing devices should be physically secured (protected). Laptops should be tethered while in use. The equipment should be locked in a cabinet, desk, or office, etc., when not in use or after hours.
  - 3.2.1.4** To the extent possible, equipment should be located in areas that have some degree of physical separation from the public and, where possible, should face away from public view. Where computers cannot be protected from public view, privacy screens are recommended. When applicable, computer screens should also face away from other employees to ensure privacy of sensitive material.

### 3.3 Remote Access

- 3.3.1** The department supervisor must approve access to UCSF computer systems from remote locations. If a remote access system utilizes a dial-up modem, it must be expressly configured to provide secure network access.
- 3.3.2** Access to UCSF's internal network from outside of its defined network perimeter must be controlled by privileged access controls. Users are not authorized to install connections such as modems, PC Anywhere, VNC, etc. Dial-in access and Virtual Private Network (VPN) connections must be strictly controlled using password authentication.
- 3.3.3** It is the responsibility of users with dial-in access and VPN privileges to ensure that non-authorized individuals do not gain access to a dial-in connection to UCSF, to UCSF sensitive information, or to internal networks. Users with remote access from personally

---

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.

# Physical Safeguards: Workstation Use Procedures

Revision B  
Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 04/11/05

owned computing devices are responsible for employing security protections equivalent to those deployed on campus.

## 3.4 Reporting Computer Security Incidents

**3.4.1 Process for Reporting Lost or Stolen Devices and/or Media:** Workforce members are required to immediately report to their department supervisor the loss or theft of any computing device on which UCSF patient or sensitive business information is stored, whether or not the hardware is owned by UCSF. The department supervisor or manager is responsible for reporting the loss/theft to UCSF Police in accordance with the Process for Reporting Lost/Stolen Device and/or Media which is available via the UCSF HIPAA Departmental Compliance website [http://www.ucsf.edu/hipaa/dept\\_compliance/](http://www.ucsf.edu/hipaa/dept_compliance/), or on the Information Technology Services website [http://isecurity.ucsf.edu/content/pdfs/Flowcart\\_A.pdf](http://isecurity.ucsf.edu/content/pdfs/Flowcart_A.pdf)

**3.4.2 Process for Reporting Hacked or Compromised Computers:** If you suspect that your computer has been hacked or compromised, report the incident in accordance with the Process for Reporting Hacked or Compromised Computers which is available via the UCSF HIPAA Departmental Compliance website [http://www.ucsf.edu/hipaa/dept\\_compliance/](http://www.ucsf.edu/hipaa/dept_compliance/), or on the Information Technology Services website [http://isecurity.ucsf.edu/content/pdfs/Hacked\\_Computers.pdf](http://isecurity.ucsf.edu/content/pdfs/Hacked_Computers.pdf)

## 4.0 Initiation and Control Reporting

## 5.0 Records & Documentation Control

## 6.0 Related Documents

Document Name	Procedure No.
---------------	---------------

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.

## Physical Safeguards: Workstation Use Procedures

Revision B

Dean's Office  
Information Services Unit  
Issue Date:  
Last Revision: 04/11/05

HIPAA Security Rules: Workstation Use Workstation Security	<b>164.310(b)</b> <b>164.308(c)</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
HIPAA Security Rules: Workstation Use Workstation Security	<b>164.310(b)</b> <b>164.308(c)</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
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)	<b>SP 800-66</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
University of California Business and Finance Bulletin IS-3 Electronic Information Security	<b>IS-3</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a> or <a href="http://www.ucop.edu/ucophome/policies/bfb/is3.pdf">http://www.ucop.edu/ucophome/policies/bfb/is3.pdf</a>
Information Security and Confidentiality Policy (UCSF)	<b>650-16</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
Medical Center Information Security and Confidentiality Policy (UCSF Medical Center)	<b>5.01.04</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>
Inventory Management Policy Personal Computer and Other IT Product Evaluation, Acquisition, Tracking and Charging Policy	<b>3.01.08</b> <b>3.02.13</b> <a href="http://manuals.ucsfmedicalcenter.org/">http://manuals.ucsfmedicalcenter.org/</a>
Mobile Device Security Recommendations (in development) Mobile Computing Guidelines Safe Computing Guidelines (in development) Proper Internet Use Guidelines (in development)	<b>60.016</b> <b>60.015</b> <b>60.017</b> <a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>

### REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A		Dan Yee and Binh Nguyen	Initial Release
B		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 02/22/05