

1.0 Purpose

The purpose of this document is to describe guidelines concerning appropriate use and security of workstations, peripheral devices, protection of confidential information, and securing unattended workstations to prevent unauthorized access.

The HIPAA Security Rules governing this procedure include:

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.

164.310(c) Workstation Security. Implement physical safeguards for all workstations that 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 the UCSF School of Nursing 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 Guidelines****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 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.

3.2 Workstation Security Guidelines: Implement the following guidelines to ensure that workstations used to access, transmit, receive or store ePHI are appropriately secured in accordance with these procedures.

- 3.2.1** A user identification and password authentication mechanism must be implemented to control user access to systems.
- 3.2.2** A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
- 3.2.3** A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.
- 3.2.4** All unused or unnecessary services must be disabled.
- 3.2.5** Workstations that are located in open, common, or

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.

otherwise insecure areas must implement the following measures:

- 3.2.5.1** An inactivity timer or automatic logoff mechanism must be implemented.
- 3.2.5.2** Workstation monitors must be situated in a manner that prohibits unauthorized viewing. The use of a screen guard or privacy screen is recommended.
- 3.2.6** Users are required to log off of applications containing patient health or sensitive business information *before* leaving their workstations. Alternatively, Windows XP users may lock their workstations using the Windows Logo Key + L.
- 3.2.7** Network file server shared drives (Personal “H:” or Departmental workgroup “O:” drives) should be used to store sensitive or critical files.
- 3.2.8** Laptops and mobile computing devices should be physically secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations throughout UCSF. Locking the equipment in a cabinet, desk, or office, etc., when not in use or after hours, may provide added security.
- 3.2.9** Workstations, which access patient health information or sensitive business information, are required to have an enabled password-protected screensaver. In cases where password-protected screen savers are not available, non-password-protected screen savers should be enabled. Exceptions to this guidance require written approval of the Chief Information Officer.
- 3.2.10** Workstations containing or accessing sensitive patient or business information should enable auto log-off capabilities if available.
- 3.2.11** All computing devices owned by the UCSF School of Nursing shall be inventoried/tagged and tracked by the Information Technology Technical Support Group.

- 3.2.12** The UCSF School of Nursing Information Technology Technical Support Group has established standard configurations for desktop technologies deployed throughout the School. All computers, computer peripherals and software as well as printers, faxes, and other miscellaneous hardware purchased with School of Nursing funds or attached to any component of the UCSF network must meet the IT Desktop Standards.
- 3.2.13** Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs (Graphic Interface Files), by employees is strictly prohibited. Software required for end user purposes must be approved and installed by IT. The end user must document and maintain proof of license to have such applications. Software installations will be coordinated through the School of Nursing IT Technical Support Group at (415) 502-8286.
- 3.2.14** Workstations must be installed with physical safeguards to eliminate or minimize the possibility of unauthorized access to information or theft of equipment.
- 3.2.15** 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 mandated. When applicable, computer screens should also face away from other employees to ensure privacy of sensitive material.
- 3.2.16** Workstations and mobile computing devices will be protected from exposure to physical threats including theft based on potential risk and available safeguards. Desktops should be physically secured to desktops, tables or walls to prevent theft. Mobile computing devices, such as notebooks and PDA's are the responsibility of the

user.

- 3.2.17** Workstations must be equipped with security hardware and/or software. Where appropriate, all workstations and portable devices must be equipped with updated software for detecting the presence of malicious software (e.g. computer viruses/worms/spyware). All computing devices must have current versions of anti-virus, anti-spyware and firewall software enabled. Operating systems must have all critical updates installed.

3.3 Mobile Computing Device Security Guidelines

- 3.3.1** Start up authentication (login ID) and authorization passwords are required on all mobile computing devices that store patient health information (PHI) or confidential data whether or not the hardware is owned by the UCSF School of Nursing. Additional passwords and/or encryption may be required at the discretion of the Information Technology Technical Support Group.
- 3.3.2** Passwords and user IDs for computer systems and networks must not be stored on mobile computing devices without encryption protection.
- 3.3.3** Approved remote access via mobile computing devices will be established by the Information Technology Technical Support Group, when necessary.
- 3.3.4** Mobile computing devices that have stored data belonging to UCSF may not be shared with others who are not authorized to access that information unless that information is stored in encrypted password-protected files.
- 3.3.5** Vendors, consultants, business associates and all others wishing to connect portable computing devices to the UCSF network must first submit the equipment to the Information Technology Technical Support Group to examine anti-virus, anti-spyware and firewall software and critical operation system updates. To initiate this process, contact the Information Technology Technical

Support Group at (415) 502-8286.

3.4 Remote Access

- 3.4.1 The department supervisor and the Information Technology Technical Support Group 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.
- 3.4.2 Access to the UCSF School of Nursing's internal network from outside of its defined network perimeter must be controlled by privileged access controls that may only be established by the Information Technology Technical Support Group. 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.
- 3.4.3 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 the UCSF School of Nursing, to UCSF School of Nursing information, or to internal networks. Users with remote access from personally owned computing devices are responsible for employing security protections that can prevent their computing device from passing along viruses or similar Internet threats to the UCSF network and data.

3.5 Reporting Computer Security Incidents

- 3.5.1 **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 PHI or sensitive business information is stored, whether or not the hardware is owned by the UCSF School of Nursing. 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/, or on the Information Technology Services website http://isecurity.ucsf.edu/content/pdfs/Flowcart_A.pdf

The loss/theft must also be reported to the School of Nursing Information Technology Technical Support Group at (415) 502-8286.

3.5.2 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/, or on the Information Technology Services website http://isecurity.ucsf.edu/content/pdfs/Hacked_Computers.pdf

Additionally, your suspicions should immediately be reported to the School of Nursing Information Technology Technical Support Group at (415) 502-8286.

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Workstation Use Workstation Security	164.310(b) 164.308(c) http://www.ucsf.edu/hipaa/dpt_compliance/
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)	SP 800-66 http://www.ucsf.edu/hipaa/dpt_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	IS-3 http://www.ucsf.edu/hipaa/dpt_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
Information Security and Confidentiality Policy (UCSF)	650-16 http://www.ucsf.edu/hipaa/dpt_compliance/
Medical Center Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dpt_compliance/
Inventory Management Policy Personal Computer and Other IT Product Evaluation, Acquisition, Tracking and Charging Policy	3.01.08 3.02.13 http://manuals.ucsfmedicalcenter.org/
Mobile Device Security Recommendations (in development) Mobile Computing Guidelines Safe Computing Guidelines (in development) Proper Internet Use Guidelines (in development)	60.016 60.015 60.017 http://www.ucsf.edu/hipaa/dpt_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A		Dan Yee and Binh Nguyen	Initial Release
B	01/02/2007	Rob Slaughter	Adapted for School of Nursing

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.