

1.0 Purpose

These procedures describe guidelines for the acceptable use of mobile computing devices and peripheral devices, protection of confidential information, and securing unattended mobile computing devices to prevent unauthorized access.

2.0 Definitions

2.1 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.

3.0 Procedures

3.1 Implement the following procedures for the acceptable use of mobile computing devices:

3.1.1 Tracking Mobile Computing Device:

Department managers and supervisors are advised to implement procedures for identifying and tracking the use of mobile computing devices, where possible.

3.1.2 Control of Physical Access To Mobile

Computing Device: Department managers and supervisors are responsible defining standards for controlling the physical access of mobile computing devices and communicating to their staff.

3.1.3 Protection Of Information: Department managers and supervisors are responsible for defining standards for controlling visible restricted or confidential information displayed on monitors or other peripherals attached mobile computing devices are restricted from unauthorized viewing.

3.1.4 Securing Unattended Mobile Computing Devices: Department managers and supervisors are responsible for defining standards and implementing methods to physically secure unattended mobile computing devices to prevent access from unauthorized entities.

3.2 Mobile Device Security Recommendations (Refer to Appendix A)

3.3 Reporting Computer Security Incidents**3.3.1 Process for Reporting Lost or Stolen Devices and/or**

Media: In accordance with the *Process for Reporting Lost/Stolen Device and/or Media*, immediately report such

events to the UCSF Police at (415) 476-1414. This process flow is available via the HIPAA Security 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

If you are traveling and your device is lost or stolen, immediately report the event to local law enforcement authorities to file a police report and then notify UCSF Police at (415) 476-1414.

3.3.2 Process for Reporting Hacked or Compromised

Computers: If you suspect that your computer has been hacked or compromised, report the incident to the Customer Support Center at (415) 514.4100, in accordance with the *Process for Reporting Hacked or Compromised Computers*. This process is available on the Information Technology Services website

http://isecurity.ucsf.edu/content/pdfs/Hacked_Computers.pdf

4.0 Initiation and Control Reporting See above

5.0 Records & Documentation Control See above

6.0 Related Documents

Document Name	Procedure No.
University of California Business and Finance Bulletin IS-3 Electronic Information Security	IS-3 http://www.ucsf.edu/hipaa/dept_compliance/ or http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
Information Security and Confidentiality Policy (UCSF Campus)	650-16 http://www.ucsf.edu/hipaa/dept_compliance/
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dept_compliance/
Workstation Use and Workstation Security Procedures	60.009 http://www.ucsf.edu/hipaa/dept_compliance/
Safe Computing Guidelines	60.015 http://www.ucsf.edu/hipaa/dept_compliance/
End User Departmental Security Standards	60.019 http://www.ucsf.edu/hipaa/dept_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	02/18/05	Carl Tianen and Ellen Amsel	Initial Release Version 1.2
B	03/16/05	Barbara Heredia	Version 1.3 Sections 3.1.1, 3.3 and 6.0
C	03/21/05	Dan Yee and Barbara Heredia	Version 1.4 Section 3.1.1 and 3.3.2
D	12/06/2006	Rob Slaughter	Revised 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.

Appendix A: Mobile Device Security Recommendations

The adoption of wireless technologies and handheld devices is becoming widespread in business, industry, and university organizations. The use of handheld devices introduces new risks to existing enterprise computing resources. Therefore, organizations require new strategies to mitigate the security risks associated with the integration of wireless technologies into existing computing environments

Introduction:

Wireless handheld devices, such as Personal Digital Assistants (PDAs), cell phones, text pagers and removable storage devices enable mobile ad-hoc networking of the workforce and provide flexible enterprise data access and electronic-commerce capabilities. While mobile computing opens new application areas, its characteristics introduce vulnerabilities to attacks varying from inadvertent actions to deliberate, aggressive interferences with corporate operations. At this time PDAs are the most precarious due to the features inherent in those devices.

At UCSF, PDAs increasingly retain protected health information, but unlike their desktop counterparts, they lie at the periphery of organizational controls and oversight. Limited computing power, memory, interfaces, and battery life impose constraints on the practicality of applying standard safeguards. The PDA's small size and mobility also leads to greater exposure to theft or misuse in the field.

Serious security concerns stem from the variety of ways in which a PDA can interact with other computing resources. These devices can inadvertently transfer malicious applications from one PDA onto another, or throughout the corporate network. Since PDA-enabled, application-level malware cannot typically be blocked by corporate firewalls, a PDA may serve as a back door through which network vulnerabilities can be exploited. In short, a PDA is exposed to multiple risks associated with external communications and interfaces over which enterprise information security organizations have no or very limited control.

To reduce or eliminate common risks associated with handheld devices, an organization must have the means to express, monitor, and enforce corporate security policy effectively, particularly over external communications and interfaces. Currently, at UCSF, the capability does not exist to enforce a policy for mobile devices.

Risk:

From a risk perspective, several major issues loom over the use of mobile devices including the following items:

- Because of their small size, mobile devices may be misplaced, left unattended, or stolen.
- User authentication (typically a password) may be disabled, a common default mode, divulging the contents of the device to anyone who possesses it.
- Even if user authentication is enabled, the authentication mechanism may be weak or easily circumvented.
- Wireless transmissions may be intercepted and, if unencrypted or encrypted under a flawed protocol, their contents made known.
- The ease with which handheld devices can be interconnected wirelessly, combined with weak or no authentication of the parties involved, provides new avenues for the introduction of viruses or other types of malicious code, and also other forms of attack such as a “man-in-the-middle attack”.

For example, a business associate can unknowingly beam a Trojan horse application from her PDA to a colleague’s PDA through an IrDA port. The victim can subsequently introduce the malware to the corporate network when he synchronizes the PDA to his desktop computer. Given that the malware was not analyzed by the corporate firewall, the PDA can inadvertently serve as a channel through which network vulnerabilities are exploited. Similarly, the user can browse the Internet using a PDA via a third party ISP and download or upload data or applications that violate the corporate security policy.

In short, the PDA has multiple access points over which the enterprise an organization cannot exercise any control or influence.

Despite the fact that security mechanisms such as data encryption and anti-virus software are becoming available for them, mobile devices typically lack sufficient controls to enforce use of the available mechanisms in accordance with a prescribed corporate security policy.

Recommendations:

Mobile devices include but are not limited to:

1. Text pagers
2. PDAs
3. Cell phones
4. Removable storage:
 - a. Memory sticks
 - b. Floppy disks
 - c. CDs

The following recommendations apply to any mobile device, including personal mobile devices when used for UCSF business:

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.

1. Consider a more secure, alternative method for storing any confidential or protected health information. UCSF protected servers should be the first option for storage of confidential or ePHI.
2. Only use devices that can restrict access by way of a password or other authentication method
3. Enable all security features the device may have
4. Store only the minimum amount of data necessary on a mobile device for the shortest time possible
5. For data that requires longer storage requirements, move it to a more secure device and delete it from the mobile device as soon as possible. UCSF protected servers should be the first option for storage of confidential or ePHI.
6. Report the loss or theft of a mobile device as soon as possible to the UCSF Police at 476-9911
7. Home computers used for UCSF business should have protection equal to that of UCSF located computers:
 - a. Proper identification and authentication to access the device to assure authorized use only
 - b. A properly configured personal firewall should be enabled
 - c. Anti-virus protection that has the latest, most current anti-virus signatures. An auto update feature that downloads updates when available is recommended.
 - d. The system should be kept current with the latest, most current operating system security patches. An auto update feature that downloads updates when available is recommended.
 - e. An anti-spy ware program from a trusted source with the latest, most current updates should be in place
 - f. Remote access to the UCSF internal network must be through approved methods only.