

1.0 Purpose

The purpose of the Transmission Security Procedures is to outline security standards for protecting the *integrity* and *confidentiality* of information that is transmitted via the UCSF network infrastructure; and for maintaining the *availability* of transmission resources, which includes protecting network infrastructure from virus attack. These procedures are governed by HIPAA Security Rules:

164.312(d)(8) Person or Entity Authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health is the one claimed.

164.312(e)(1) Transmission Security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

2.0 Definitions

2.1 Encryption: Translating data or documents into a code that cannot be read without a "key." Encryption is the best way to ensure that e-mail is not intercepted and tampered with between the time it is sent and the time it is received.

2.2 Encryption levels: Examples of two levels of encryption are: 40-bit and 128-bit. With 40-bit encryption, there are billions of possible keys to decipher the coded information, but only one of them works. With 128-bit encryption, there are 300 billion trillion times as many keys as with 40-bit encryption.

2.3 IPsec: Internet Protocol Security. IPsec uses encryption technology to provide data confidentiality, integrity, and authenticity between participating peers in a private network.

2.4 Workforce: All faculty, staff, students, trainees, volunteers, and business associate who access restricted or confidential information during the course of their duties.

3.0 Procedures

3.1 Confidential transmissions to networks outside of the UCSF network: To appropriately guard against unauthorized access to or modification of confidential data that is being transmitted from the UCSF network to a network outside UCSF, the procedures outlined in this section must be implemented.

3.1.1 All confidential transmissions from UCSF to a network outside of the aforementioned network must utilize

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.

an encryption mechanism between the sending and receiving entities; or the file, document; or folder containing said confidential data must be encrypted before transmission.

3.1.2 Prior to transmitting confidential information from UCSF to a network outside of the aforementioned network, the receiving person or entity must be authenticated.

3.1.3 All transmissions of confidential information from UCSF to a network outside of the aforementioned networks should include only the minimum amount of information necessary.

3.1.4 For transmission of confidential information from UCSF to a network outside of the aforementioned networks utilizing an email or messaging system, see section 3.3 below.

3.2 Confidential Transmissions Using Electronic Removable Media

3.2.1 When transmitting confidential information via removable media, including but not limited to, floppy disks, CD ROM, memory cards or memory sticks, magnetic tape and removable hard drives, the sending party must:

3.2.1.1 Use care to ensure that the information is protected against unauthorized disclosure.

3.2.1.2 Authenticate the person or entity requesting said ePHI in accordance with HIPAA Security Rule and UC policy.

3.2.1.3 Send the minimum amount of confidential information required by the receiving person or entity.

3.2.1.4 If using removable media for the purpose of system backups and disaster recovery, and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

3.3 Confidential Transmissions Using Email or Messaging Systems

3.3.1 The transmission of confidential information from UCSF to a recipient via an email or messaging system is

permitted only via UCSF School of Nursing approved and supported secure email solutions.

3.3.2 The transmission of confidential information from UCSF to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

3.3.2.1 The receiving entity has been authenticated.

3.3.2.2 The receiving entity is aware of the transmission and is ready to receive said transmission.

3.3.2.3 The sender and receiver are able to implement a compatible encryption mechanism.

3.3.2.4 All attachments containing confidential information are encrypted.

3.4 Confidential Transmissions Using Wireless LANs and Devices

3.4.1 The transmission of confidential information over a wireless network within the UCSF Medical Center or UCSF domains is permitted if the following conditions are met:

3.4.1.1 The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized.

3.4.1.2 The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

3.4.1.3 If transmitting confidential information over a wireless network that is not utilizing an authentication and encryption mechanism, the ePHI must be encrypted before transmission.

3.4.1.4 The authentication and encryption security mechanisms implemented on wireless networks within the UCSF Medical Center domain is only effective within the Medical Center network. When transmitting outside of the Medical Center wireless network, additional and appropriate security measures must be implemented in accordance with this procedure.

3.5 Additional Requirements

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.

- 3.5.1 All encryption mechanisms implemented to comply with this procedure must support a minimum of 3DES standard, but not limited to, 128-bit encryption.
- 3.5.2 When transmitting confidential information regardless of the transmission system being used, workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the information requested.

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Person or Entity Authentication Transmission Security	164.312(d)(8) 164.312(e)(1) 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 Campus)	650-16 http://www.ucsf.edu/hipaa/dpt_compliance/
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/dpt_compliance/
Security Management Procedures Information Access Management Procedures	60.001 60.003 http://www.ucsf.edu/hipaa/dpt_compliance/

REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	03/07/05	Dan Yee, Binh Nguyen	Initial Release
B	03/18/05	Dan Yee	Version 1.5 sections 3.2.1.1
C	01/02/07	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.

Does not include changes after 01/02/2007