University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 9.13

Title:	**Security of E-PHI on Home Computers**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**04/03/05**
Applies:	**All UCD campuses**

Introduction

Purpose

The purpose of this policy is to provide general guidelines to ensure security of electronic Protected Health Information (ePHI) on home computers and when accessing ePHI on the UCD network from home.

Reference

Remote Access Service via High Speed Internet Access Policy

Applicability

This policy applies to the downloading of ePHI data and/or software to home computers by members of the UCD workforce. This policy is applicable whether the computer is owned by UCD or the user. This policy also applies when a member of the UCD workforce uses a home computer to access ePHI on the UCD network.

Policy

All members of the UCD workforce who download ePHI to home computers or who use home computers to access ePHI on the UCD network shall follow this policy.

Procedures

A. <u>Access of ePHI from Home Computers Owned by UCD</u>

Before connecting to the UCD network via remote access, the home computer user must:

1. Complete the appropriate remote access request form. See Reference section above.

2. Install and keep up-to-date the campus standard anti-virus software to prevent the spread of malware (viruses/Trojans, etc.);

3. Apply critical security patches for operating systems and applications and keep patches up-to-date;

4. Install anti-spyware software, keep it up-to-date, and run software on a regular basis, no less than monthly;

5. No non-work-related software is to be installed on a computer owned by UCD;

6. If connection to the Internet is via a high-speed connection (i.e. cable-modem, DSL, satellite, etc.), firewall software must be installed and set up to allow only trusted IP addresses;

7. Care must be taken when accessing web sites; many websites harbor malware. Anti-spyware software should be run after leaving a site whose security may be suspect;

8. If the home computer is part of a home network, if at all possible, do not download ePHI to the computer. Home networks introduce greater risk of unauthorized access to the data; and,

9. If the home computer is part of a wireless home network, if at all possible, do not download ePHI to the computer. Wireless networks set up with default wireless encryption are insecure. If it is necessary to download ePHI to the home computer, ensure that the latest wireless security is in place. Currently that means installing WPA (Wi-Fi Protected Access) on the home computer.

B. <u>Access of ePHI from Home Computers Not Owned by UCD</u>

Before connecting to the UCD network via remote access, the home computer user must follow all steps above except for the prohibition against installing non-work-related software.

C. <u>Download of ePHI to Home Computers</u>

Extra care must be taken if ePHI is downloaded or copied onto home computers.

1. ePHI should not be downloaded or copied onto home computers without prior written approval from the data owner.

2. ePHI stored on the home computer must be encrypted to protect against unauthorized access.

3. If ePHI must be transmitted across the Internet via e-mail, use of the UCD e-mail system and secure e-mail procedures are required.

4. If ePHI must be transmitted across the Internet via any means other than e-mail, the ePHI must be encrypted prior to transmission or a secure connection must be made.

5. When the ePHI is no longer needed on the home computer, it must be completely removed from the computer. After deleting the files, the Windows Recycle Bin or Macintosh Trashcan must be emptied.

6. If the home computer stores ePHI and is stolen the user must notify the Office of HIPAA Compliance as soon as the theft is discovered.

7. If the home computer contains or contained ePHI and becomes non-functional or is to be replaced, the ePHI must be permanently destroyed prior to disposing of the computer. If the computer is functional, use a disk wiping tool to permanently destroy the ePHI. If the computer is non-functional, remove the hard drive and destroy it either by smashing or puncturing it.