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 9.11

Title:	**Portable Media Security**
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:	**04/04/05**
Applies:	**All UCD campuses**

Introduction

Purpose

The purpose of this policy is to establish guidelines for secure use of portable media and protection of any ePHI (electronic Protected Health Information) stored on portable media.

Reference

N/A

Applicability

This policy applies to the use of all types of portable devices that may be used to store ePHI. Portable media can include, but is not limited to, laptops, mobile devices such as personal digital assistants (PDAs) or other types of wireless handheld devices, USB flash drives, memory sticks, and any other portable device used to store or transport data.

Policy

All PHI stored on portable media shall be protected in accordance with this policy.

Procedures

A. General

1. If at all possible, do not store ePHI on portable media.
2. If it is necessary to store ePHI on portable media:

   a. Password protect the device using a complex password;

   b. Encrypt the ePHI stored on the device using the campus-provided encryption software;

   c. Store only the minimum necessary ePHI if the purpose of storing the ePHI is not for treatment, payment, or healthcare operations;

   d. When it is no longer necessary to store the ePHI on the device:

      i. If the device will continue in use, delete the ePHI and empty the recycle bin or trash can;

      ii. If the device will continue to be used but none of the data stored on the device will be needed again, use a disk wiping tool to remove all traces of all data stored on the device; or

      iii. If neither the device nor the data stored on the device will be used again, destroy the device by breaking or puncturing it.

e. If the device is lost or stolen, report this as soon as possible to the ITS Help Desk.