STORAGE AND USE OF RESTRICTED INFORMATION ON MOBILE DEVICES AND REMOVABLE MEDIA

PURPOSE
Mobile Devices and Removable Media such as laptops and USB storage drives are increasingly useful electronic tools for communication and patient, education, and research management. They are also at high risk for loss or theft. The purpose of this policy is to protect the confidentiality of University documents, proprietary University data, and individually identifiable information, by requiring encryption and password protection of all types of Mobile Devices and Removable Media used for any University Business.

SCOPE
This Policy applies to all faculty, staff, employees, students and trainees of the Ronald Reagan UCLA Medical Center, the Santa Monica UCLA Medical Center and Orthopaedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics and the David Geffen School of Medicine at UCLA.

DEFINITIONS
“Encryption” means the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. While encryption requires a password or other means to decrypt the information, a password on a mobile device does not mean the device is encrypted.

“Mobile Devices” include but are not limited to laptops, cell phones, smart phones (IPhones, Blackberry, Droid, etc.), tablet computers, iPads, and PDAs.

“Removable Media” includes but is not limited to USB (flash, thumb) drives, external hard drives, CDs, DVDs, and magnetic tape.

“Restricted Information” (as defined by University of California Policy IS-3, Electronic Information Security) describes any confidential or Personal Information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. This includes Personal Information, Protected Health Information, ePHI as defined in UC Policy IS-3, and research data.

“University Business” means any activity associated with the performance of one’s duties as any employee, trainee, or volunteer, at any time of day or from any location.
University Business includes but is not limited to note-taking, reviewing and drafting documents and presentations, accessing University e-mail through any method, documenting medical services, and recording or storing research data.

A. POLICY
A. All Mobile Devices and Removable Media used by any individual covered under this Policy for University Business must be encrypted and password protected.

B. One of the following will be required to validate that a mobile device has been properly encrypted and password protected.

   I. Laptops:
      a. If the laptop was issued by the UCLA Health Sciences IT Organization, it will be encrypted, password protected and have a control sticker indicating that encryption has been enabled on the device.
      b. If the laptop was purchased either by an individual employee or by his/her local operating unit encryption and password protection must be confirmed and the laptop inventoried by the UCLA Health Sciences IT Organization.
      c. If the laptop was purchased by an individual employee and he/she has enabled the built-in encryption program of the operating system, a screen shot must be submitted to the UCLA Health Sciences IT Organization demonstrating that the encryption and password protection has been enabled.
      d. Other acceptable means as defined or approved by the Office of Compliance Services- Information Security in conjunction with the Health Sciences IT Organization. Such approval must be documented in writing.

   II. Other Mobile Devices including cell phones and tablets must have Airwatch enabled such that the device can be identified by Information Services and Solutions (ISS).

C. All Removable Media devices must be encrypted. Individuals covered under this Policy will be required to produce evidence of encryption if his or her Removable Media is lost or stolen.
D. Passwords for encrypted Mobile Devices and Removable Media must conform to the policies and procedures described in HS Policy No. 9452, “User Accounts (Authorizing Access to Restricted Information; Passwords).”

E. Requirements on separation from the University:

I. Restricted Information may not be taken with an individual on separation from UCLA without written permission from an appropriate UCLA authorizing party.

II. All UCLA property must be returned to the individual’s Department prior to or at the time of separation.

III. All Restricted Information must be deleted from non-University owned Mobile Devices and Removable Media.

F. If Restricted Information on a Mobile Device or Removable Media used for University business has been lost, stolen or otherwise compromised, individuals covered by this policy must immediately notify his/her Department Administrator and the Office of Compliance Services (PrivacyInfoSec@mednet.ucla.edu).

G. Certain individuals covered by this policy may be required to submit an attestation to the University acknowledging their obligations under this Policy.

H. Sanctions:

I. Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination. (See: HS Policy No. 9461, “Privacy and Information Security Sanctions.”)

II. Departments will bear financial responsibility for costs incurred as a result of any failure of the Department, or any failure of a faculty member or employee of the Department, to adhere to the requirements of this policy. Individuals could bear financial responsibility for their failure to adhere the requirements of this policy.
REFERENCES
Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 et seq.
California Civil Code Sections 1798.29 and 1798.82
California Health and Safety Code Section 1280.15
UCLA Policy No. 404, Protection of Electronically Stored Information
Office for Civil Rights, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Undecipherable
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidanc e.html
National Institute of Standards and Technology, Guide to Storage Encryption Technologies for End User Devices

CONTACT
Chief Privacy Officer, Office of Compliance Services
Chief Information Security Officer, Office of Compliance Services

REVISION HISTORY
Approved: April 8, 2003; February 22, 2006
Effective Date: April 14, 2003; April 20, 2005,
Review Date: July 25, 2012, January 28, 2015, September 24, 2015
Revised Date: June 30, 2004; April 8, 2005; November 2005; June 21, 2007; May 30, 2008,

Formerly Policy No. 9452, “Collection and Use of Patient Identifiable Health Information On PDAs, Laptops, And Other Portable Computing Devices”

APPROVAL
Health Sciences Enterprise Compliance Oversight Board
Approved 9/24/2015

John Mazziotta, M.D., Ph.D.
Vice Chancellor, Health Sciences & Dean, School of Medicine
UCLA Health System
Shannon O’Kelley,
Interim Vice President and COO
UCLA Health System

Patricia A. Kapur, M.D.
Executive Vice President, UCLA Health System
UCLA Faculty Practice Group

Earl G. Freymiller, M.D., D.M.D.
Chief of Staff
Ronald Reagan UCLA Medical Center

Roger M. Lee, M.D.
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic Hospital

Robert Suddath, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA