Future version of HS Policy No. 9453-C – Effective on 12/31/17
Device and Removable Media Encryption

Purpose

Workstations, Mobile Devices and Removable Media are routinely used electronic tools for communication, patient care, education, and research. They are also at risk for loss or theft, especially Mobile Devices. 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 Workstations, 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, Android, 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.

*"**Workstation**"* means a desktop computer.

*"**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.

POLICY

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

II. Workstations that are not UCLA-owned that meet the requirements below may be excepted from this policy:

   A. The only University Business use of the Workstation is for CareConnect remote access, Outlook Web Access, Windows Remote Desktop or other functions listed in the Health Sciences Device Encryption Standard.

   B. No University Business documents are ever stored, even temporarily, on the Workstation.

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

   A. Workstations and Laptops:

      1. If the computer was issued by the UCLA Health Sciences IT Organization, it will be encrypted and password protected.

      2. If the computer was purchased either by an individual employee or by his/her local operating unit encryption and password protection must be confirmed and the computer inventoried by the UCLA Health Sciences IT Organization.

      3. If the computer was purchased by an individual employee and he/she has enabled the built-in encryption program of the operating system, the encryption of the computer must be registered with the UCLA Health Sciences IT Organization to provide documentation of encryption.

      4. 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.

   B. Other Mobile Devices including cell phones and tablets must have Airwatch enabled to confirm encryption and allow the device to be identified by Information Services and Solutions (ISS).

IV. 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.

V. Passwords and other authentication credentials for encrypted Workstations, 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)."

VI. Requirements on separation from the University:

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

   B. All UCLA property must be returned to the individual's Department prior to or at the

time of separation.

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

VII. If Restricted Information on a Workstation, 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).

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

IX. Any additional technical requirements of the Health Sciences Device Encryption Standard must also be followed.

X. Sanctions:

A. 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.*")

B. 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 to the requirements of this policy.

XI. Questions

A. For any questions on how to encrypt a device or register a computer as encrypted, contact your IT Support group.

B. For questions on this policy, contact the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu)

XII. Exceptions

Any exceptions to this policy must be for a compelling patient care or business reason and must be approved by the Chief Compliance Officer or his/her designee. The Chief Compliance Officer or designee will consult with the appropriate business, leadership and IT groups in evaluating any proposed exceptions. Exceptions may be requested by submitting an exception request form which may be obtained by emailing InfoSecAll@mednet.ucla.edu.

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/brguidance.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf
National Institute of Standards and Technology, Guide to Storage Encryption Technologies for End User Devices
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

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, March 31, 2011, October 25, 2012, February 27, 2015, September 24, 2015

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

Formerly "Storage and Use of Restricted Information on Mobile Devices and Removable Media Policy"

APPROVAL

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

John Mazziotta, M.D., Ph.D.
Vice Chancellor, UCLA Health Sciences
Dean, David Geffen School of Medicine

Shannon O'Kelley,
Interim Vice President and COO
UCLA Health System

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