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

PURPOSE

To establish a policy for the storage and use of Restricted Information on mobile devices (including but not limited to laptops, cell phones, tablet computers, personal digital assistants ("PDAs"), USB drives and external hard drives), removable storage media or other non-network secured resources in order to safeguard confidentiality and to meet applicable state and federal laws and regulatory standards. This policy applies to the UCLA Heath System and David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health").

DEFINITIONS

"Protected health information" or "PHI" is any individually identifiable health information, in any format, including verbal communications. "Individually identifiable" means that the health or medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes patient billing and health insurance information and applies to a patient's past, current or future physical or mental health or treatment.

"Electronic Protected Health Information" or "ePHI" is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

"*Personal Information (PI)*" as used in this policy is an individual's first name or first initial and last name combined with any one of the following:

(1) social security number,
(2) driver's license number or California identification card number,
(3) account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account,
(4) medical information, or
(5) health insurance information.

"Medical information" means any information, in either electronic or physical form, regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor. "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Medical information and health insurance information for patients are also considered to be PHI.

"Restricted Information" (as defined by UC 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, PHI and ePHI as defined in this section but could also include other types of information such as research data.

"Mobile Devices" include but are not limited to laptops, cell phones, smart phones (IPhones, Blackberry, Droid etc.), tablet computers, iPads, PDAs, USB (flash, thumb) drives, and external hard drives.

"Removable Media" includes but is not limited to CDs, DVDs, magnetic tape, typewriter ribbons and cartridges.

POLICY

I. Data and files containing Restricted Information should be secured and stored on UCLA Health mainframe or network drives and servers.

II. All Restricted Information should be removed from data and files before they are stored on mobile devices or removable media.

III. Restricted Information in the custody or control of UCLA Health workforce must not be stored on mobile devices or removable media unless all the conditions below are satisfied:
   A. There is a compelling patient care, business or academic need.
   B. The device or removable media is UCLA owned, purchased and/or issued.
   C. Only the minimum necessary amount of Restricted Information is stored on the device or removable media.

D. The Restricted Information is encrypted or other approved security measures have been implemented to protect the restricted information from loss or theft of the data and/or System.

IV. Data containing Restricted Information must never be stored on a non-UCLA-owned computer, mobile device or removable media unless the user has been granted an exception to this policy.
Workforce members must return all UCLA property including Restricted Information, mobile devices and removable media before they terminate from UCLA Health. UCLA Restricted Information may not be taken with an individual when he/she terminates from UCLA Health unless written permission has been obtained from an appropriate UCLA Health authorizing party.

V. Department and program managers are responsible for ensuring that the policy requirements above are met.

VI. The provisions of sections III and IV above are not applicable to Restricted Information in email stored on cell phones or smart phones whether UCLA owned or personally owned. Storage of Restricted Information on such devices must meet the following provisions.

A. There is a compelling patient care, business or academic need and;
B. A passcode is set on the device, and
C. The passcode is not shared with anyone else, and;
D. If the device can support encryption of locally stored email, attachments and other data, the user has enabled this feature and;
E. The user must alert the Office of Compliance Services if the device is lost or stolen.

PROCEDURE / GUIDELINES

I. The transmission of Restricted Information to and from the mobile device or removable media must be performed in a secure manner in accordance with UCLA Health policies and procedures. *See*: HS Policy 9457, "*Minimum Security Standards for Network Devices*."

II. **Restricted Information on UCLA-owned** mobile devices or removable media:

A. If a user or department has a requirement to collect, store and/or process data containing Restricted Information on a UCLA-owned mobile device or removable media, all criteria defined in this policy for such devices must be met.

B. In cases where Restricted Information on a UCLA-owned mobile device or removable media cannot be encrypted or otherwise secured UCLA Health will mirror the provisions of UCLA Policy No. 404, "*Protecting Electronically Stored Information*," and require a policy exception be obtained from the Vice Chancellor of the Health Sciences. The request must describe the circumstances justifying an exception and the proposed compensating controls providing equal or greater security for the Restricted Information**.**

III. Exceptions to Policy

A. If a user or department has a requirement to collect, store and/or process data containing Restricted Information on a non-UCLA-owned mobile device or removable media then, prior to collecting, storing or processing such information on the non-UCLA-owned device, the user or department must obtain an exception to this policy from the Office of Compliance Services – Information Security except for cell phones and smart phones.

B. An exception request form must be completed. The form must first be submitted to the Department Administrator. If the Department Administrator finds that the request establishes a compelling patient care, business or academic need, he/she will recommend approval and forward it to the Office of Compliance Services - Information Security.

C. The Office of Compliance Services - Information Security, in consultation with the Office of Compliance Services - Privacy, will review the request. The following criteria will be the general basis for evaluating the request:

a. Has the requestor demonstrated a compelling patient care, business or academic need to collect, store or process Restricted Information on a non-UCLA owned mobile device or removable media?

b. What are the reasons the Restricted Information cannot be stored on a UCLA-owned server, mobile device or removable media to meet the patient care, business or academic need?

c. Is the requestor authorized to maintain the data?

d. How will the Restricted Information on the mobile device or removable media be encrypted or otherwise protected?

e. Does the mobile device or removable media have sufficient security safeguards for the protection Restricted Information?

f. Will the requestor allow the Office of Compliance Services to audit the personally-owned device or removable media?

g. What is the plan to return the Restricted Information to a UCLA-owned server, mobile device or removable media when the requestor is no longer engaged in activities for UCLA Health?

h. Is the Restricted Information on the personally-owned device original source data and if so what is the backed up, disaster recovery, business continuity, etc. plan?

i. Other appropriate considerations based on the requestor's needs and the nature of the Restricted Information.

D. The Office of Compliance Services - Information Security will either:

a. Request additional information from the requestor if the information provided is not sufficient to make a recommendation:

b. Make a recommendation to the business unit representative on the Health Sciences Enterprise Compliance Oversight Board to either approve or deny the policy exception.

IV. All UCLA Health UCLA-owned mobile devices or removable media that contain restricted information must be encrypted.

V. AES 128-bit or better encryption must be used for encryption of Restricted Information on mobile devices or removable media (*see*: Office for Civil Rights *"Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Undecipherable"*). Complex passwords or passphrases should be used.

VI. Passwords for encrypted devices must be properly secured. Passwords for access to encrypted information should not be stored with or near the device.

VII. Users must keep track of their mobile devices and removable media to ensure they are not misplaced and that unauthorized individuals do not have access to the device or the Restricted Information contained on the device.

VIII. Workforce members who are authorized to maintain Restricted Information including PHI pertaining to UCLA Health System patients on a mobile device must guard against the unauthorized use or viewing of the Restricted Information on the device.

IX. Any critical data on mobile devices must be backed up in a secure manner and at an appropriate frequency based on the nature of the data.

X. Before replacing or disposing of mobile devices or removable media containing Restricted Information, the user must securely wipe or overwrite the data (*see*: HS Policy No. 9456, *"Physical Security"*).

XI. If the user has any reason to believe the data on a mobile device or removable media has been compromised, the user must immediately notify his/her Department Administrator and the Privacy and Information Security Offices (PrivacyInfoSec@mednet.ucla.edu).

XII. **Questions**
Any questions on storing Restricted Information on mobile devices or removable media should be referred to the user's IT support group or the Privacy and Information Security Offices (PrivacyInfoSec@mednet.ucla.edu).

XIII. **Enforcement**
Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination.

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
Revised Date: June 30, 2004; April 8, 2005; November 2005; June 21, 2007; May 30, 2008, March 31, 2011, October 25, 2012

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 6/27/12

David Feinberg, M.D.
CEO and Associate Vice Chancellor
UCLA Hospital System

Kevin M. Shannon, M.D .
Chief of Staff
Ronald Reagan UCLA Medical Center

Denise Sur, M.D.
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic hospital

Ian A. Cook, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA