Current Status: *Active* **PolicyStat ID:** *4995236*

Effective Date:	*4/20/2005*
Review Date:	*7/30/2018*
Revised Date:	*7/30/2018*
Next Review:	*7/29/2021*
Owner:	*Ann Chang: Dir*
Policy Area:	*Compliance*
Reference Tags:	
Applicability:	*Ronald Reagan UCLA Medical Center* *Ambulatory Care - UCLA* *Resnick Neuropsychiatric Hospital* *Santa Monica UCLA Medical & Orthopaedic* *UCLA Health*

Ronald Reagan UCLA Medical Center

Physical Security of Restricted Information Policy, HS 9456

PURPOSE

This policy sets forth guidelines by which UCLA Health Sciences shall select appropriate mechanisms to physically safeguard Restricted Information in any form, including, but not limited to computing devices, electronic storage media, paper, and any other devices that store, transmit or access Restricted Information.

SCOPE

This Policy applies to all faculty, staff, employees, students, trainees, and volunteers 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 (hereafter referred to as "UCLA Health Sciences").

In addition, it applies to suppliers, contractors and other non-workforce members who are allowed access to UCLA Health Sciences Electronic Information Resources or Restricted Information and to any devices, including personally owned devices that store Restricted Information.

POLICY

I. Physical access to systems containing Restricted Information must be controlled as carefully as possible. Computers which are housed in leased property or which are accessed by contract cleaning and maintenance services need to be carefully secured. Access to secure locations should be limited to authorized users only, and logs to track ingress and egress from locations should be maintained.

II. Large enterprise system servers containing Restricted Information should be physically located in professionally managed secure locations that have provisions for the prevention, detection, early warning of and recovery from emergency conditions.

III. Smaller systems such as departmental servers, to the extent possible, should be stored in data centers, secured equipment rooms, locked offices or in other areas with limited or restricted access. Keys to the server areas should be tightly controlled and distributed only to a limited number of staff.

IV. Desktops and laptops are by definition not housed in secure areas, and therefore unencrypted Restricted Information should not be stored on desktops or laptops if a network server is available. (See: HS Policy No. 9451, "*Use of Electronic Information by Workforce.*")

V. Secure physical access locations must limit access to authorized users and have physical access controls such as locks, electronic key readers, or other access control mechanisms. UCLA Health Sciences should maintain logs to track ingress and egress (with the exception of routine daily activities).

VI. UCLA Health Sciences shall log all systems maintenance services.

VII. Wireless network access points should be protected from unauthorized access and transmissions should be encrypted (*see*: HS Policy No. 9457, *"Information Technology Security"*).

VIII. Where feasible, laptops, mobile devices and unencrypted workstations should be physically secured with cables or other lockdown devices.

IX. Access to non-public areas with servers and workstations containing Restricted Information should be limited to staff who are assigned to work in that area, or with a job-related reason for being in the area. Visitors and vendors to these areas should wear appropriate identification badges, and should be accompanied by UCLA Health Sciences staff at all times. UCLA Health Sciences should maintain logs to track visitors and vendors entering and exiting the non-public areas.

X. Individuals physically accessing UCLA Health Sciences computer resources should be requested to provide a valid UCLA Health Sciences Identification badge.

XI. Physical access to Restricted Information in paper and other formats should be controlled in a similar manner as for electronic devices. HS Policy No. 9401, *"Protection of Patient Information"* lists additional physical security measures for PHI, many of which are also applicable to Restricted Information.

XII. Devices and media containing Restricted Information must always be disposed of securely.

PROCEDURE

I. **Data Centers and Other Secure Locations**

A. UCLA Health Sciences servers containing Restricted Information should be physically located in professionally managed secure locations that have provisions for the prevention, detection, early warning of and recovery from emergency conditions created by earthquake, fire, water, leakage or flooding, power disruption, air conditioning failure, or other hazards.
To the extent possible, servers should be stored in secure data centers or equipment rooms.

B. UCLA Health Sciences should record any maintenance repairs and modification to physical components of the facility related to security such as hardware, walls, doors and locks.

C. UCLA Health Sciences should record any relocation of hardware and electronic media. UCLA Health Sciences should ensure the backup of any data before a relocation of equipment. UCLA Health IT is responsible for maintaining records for hardware and software.

D. Outside approved data centers, reasonable technical and security measures should be implemented to secure UCLA Health Sciences data and systems. A Business Associate Agreement must be executed for all outside third party data centers storing ePHI. When Restricted Information is involved, language to protect the confidentiality, integrity and availability of the Restricted Information should be included in contracts.

II. **Workstation Security**

1. **Workstation Use**.
   1. Workstations containing Restricted Information or which are utilized to access the UCLA Health Sciences network must be secured with a password.
   2. If Workforce members step away from their workstation, they must log-off the applications and invoke a screensaver lock function. This also applies to home computers utilizing VPN to access UCLA Health Sciences systems.
   3. Workstations must automatically invoke a password-protected screensaver after15 minutes of inactivity. Requests for longer time outs must be approved by the Chief Compliance Security Officer. Workstations in areas where the public may see the Restricted Information should be set up to "Timeout" after shorter periods of inactivity.
   4. Once the screensaver is invoked, the Workforce member must re-authenticate with his/her User ID and password to access the workstation.
2. **Workstation Location**.
   1. Workstations should be positioned so that unauthorized individuals cannot readily view them. Workforce members should also position any mobile devices so that the screens are not visible to unauthorized individuals or the public when in use. As much as possible, privacy screens should be utilized in areas accessible by the public.
   2. As much as possible, workstations and laptops located in an open office environment should be physically secured with anti-theft devices, such as locking cables, placed in locked cabinets, or secured via other locking mechanisms.
   3. Workstation loss or theft must be reported immediately to UCLA Health IT Customer Care at (310) 267-CARE (x7-2273), the Office of Compliance Services - Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu), and the user's supervisor. Any thefts must also be reported to the UCLA Police Department. (See: HS Policy No. 9459, "*Privacy and Information Security Incident Reporting*").
   4. Workstations in an open office environment or in areas accessible to the public must not be left unattended unless securely locked.

III. **Device and Media Controls and Accountability**

1. UCLA Health IT is responsible for maintaining inventory records for computing equipment. To the extent possible, such records should contain the names of the individuals to whom the equipment has been assigned.
2. The responsible parties should maintain inventories of electronic media (DVD/CDs, USB drives, magnetic tape, etc.) that contain Restricted Information.
3. Hardware that contains Restricted Information should not be sent out of the facility for service without the appropriate safeguards.
4. Leased or vendor equipment that contains Restricted Information should not leave the premises before all the Restricted Information has been securely deleted (see below) or other arrangements for secure disposal have been made with the vendor.
5. Hardware or media that contains Restricted Information should not be recycled, sold, or donated unless all Restricted Information is first securely deleted. Workstation, laptops and hard drives should not be re-issued to other users without first securely deleting all Restricted Information on the devices that the new user does not need to perform his/her duties.

6. Contact the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu) for information on how to securely delete Restricted Information.

IV. Secure Disposal

1. All devices and media containing Restricted Information should be disposed of securely.
   a. Workforce members can call UCLA Health IT Customer Care at (310) 267-CARE (x7-2273) to arrange for pick up of devices and media containing Restricted Information for secure disposal.
   b. Contact the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu) for information on how to dispose of media and hardware securely.
2. The only approved secure disposal method for paper Restricted Information is cross-cut shredding. Depositing the documents in a locked shredding container the contents of which will be shredded by a UCLA Health Sciences certified third party vendor will meet this requirement.
   a. Paper documents with Restricted Information must never be discarded in recycling bins or regular trash cans.
   b. Collection bins for paper documents with Restricted Information that will later be shredded should be locked.
   c. Workforce members should ask their supervisors for instructions on disposing of paper documents with Restricted Information in their areas.

V. Media Re-use

1. Restricted information stored on any electronic devices or media must be securely deleted before the devices or media can be re-used. Hard drives should not be reused unless all the Restricted Information is first securely deleted. Backup tapes from one area should not be re-used in another until they have been securely wiped.
2. Contact UCLA Health IT Customer Care at (310) 267-CARE (x7-2273) or the Office of Compliance Services - Information Security (InfoSecAll@mednet.ucla.edu) for information on how to dispose of media and hardware securely.

VI. Data Backup and Storage

If the only copy of Restricted Information is on hardware or electronic media to be moved, an exact retrievable copy of the Restricted Information should be created before moving the hardware or electronic media.

VII. Enforcement

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

VIII. Policy Exceptions

Any exceptions to this policy must be for a valid 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.

IX. Questions

Consult your supervisor, IT support group or the Office of Compliance Services Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu) if you have any questions on this policy.

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 *et seq.*
Information Practices Act of 1977, California Civil Code Sections 1798.29 and 1798.82
California Health and Safety Code Sections 1280.15, 123148 and 130203
California Lanterman-Petris Short Act ("LPS Act")
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Electronic Communications Policy (ECP)

CONTACT

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

REVISION HISTORY

Approved:	February 22, 2006
Effective Date:	April 20, 2005
Revised Date:	November 2005; June 21, 2007; May 30, 2008, March 31, 2011, July 30, 2018

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010

Johnese Spisso, RN, MPA
President UCLA Health
CEO UCLA Hospital System

Carlos Lerner, 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

Laurie R. Casaus, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA

Appendix I – Definitions

"Electronic Information Resources" includes, but is not limited to, computer equipment (servers, workstations, laptops and other portable computers), online services, medical devices, mobile devices (tablets ,smart phones, digital cameras, etc.), applications (Electronic Health Record, email, databases, other software), storage media (USB drives, DVDs, CDs, magnetic tape, memory cards), and networks.

"Protected health information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper, or oral. "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, genetic or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes medical information; 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 means either of the following:

A. An individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted:
    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, or
    6. information or data collected through the use or operation of an automated license plate recognition system as defined in the California Civil Code §1798.90.5; or

B. A user name or email address, in combination with a password or security question and answer that would permit access to an online account

"***Medical Information***" means any individually identifiable 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.

"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.

"Device" means a computer, printer, wireless appliance, or other piece of equipment that can connect to and communicate over any UCLA network or creates, receives, maintains or transmits UCLA Health Sciences Restricted Information at any location. Devices would include, but are not limited to, laptops, tablets, smart phones, servers, and medical and other devices with network connectivity.

"Server" is a Device that provides some service for other Devices connected to it via the network.

"Workstation" is defined for the purposes of this policy as a UCLA Health Sciences desktop or laptop computer.

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval	Johnese Spisso: Ceo Med Ctr [MW]	7/30/2018
Administration Approval	Carlos Lerner: Assoc Prof Of Clin-Hcomp [MW]	7/30/2018
Administration Approval	Roger Lee: Hs Clin Prof-Hcomp [MW]	7/30/2018
Administration Approval	Laurie Casaus: Hs Assoc Clin Prof-Hcomp [MW]	7/30/2018
Executive Medical Boards - MSEC, RNPH PSEC, SMEMB	M. Lynn Willis: Mgr	7/30/2018
Hospital System Policy Committee Chair	M. Lynn Willis: Mgr	7/11/2018
Hospital System Policy Committee	M. Lynn Willis: Mgr	7/11/2018
	Ann Chang: Dir	5/26/2018

Applicability

Ambulatory Care - UCLA, Resnick Neuropsychiatric Hospital, Ronald Reagan UCLA Medical Center, Santa Monica UCLA Medical & Orthopaedic, UCLA Health