Current Status: *Active* **PolicyStat ID:** *8266068*

Effective Date:	*04/2005*
Approved Date:	*07/2020*
Revised Date:	*07/2020*
Next Review:	*07/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Remote Access Policy, HS 9453-D

PURPOSE

UCLA Health Sciences networks contain confidential information, as well as critical applications and infrastructure. The Workforce, business partners, research collaborators and others have legitimate needs to access those internal electronic resources from remote locations. The purpose of this policy is to protect confidential information and resources by setting forth requirements for providing secure remote access into UCLA Health Sciences networks.

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 Orthopedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics, the David Geffen School of Medicine, UCLA School of Nursing, UCLA School of Dentistry, and UCLA Fielding School of Public Health (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.

DEFINITIONS

"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:

1. 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:
    - A. social security number,
    - B. driver's license number or California identification card number,
    - C. 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,
    - D. medical information,
    - E. health insurance information; or
    - F. information or data collected through the use or operation of an automated license plate recognition system as defined in California Civil Code §1798.90.5; or
2. 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.

"***Authentication Credential***" is something such as a password, biometric identifier (for example, a fingerprint, iris scan, or voiceprint), certificate, security token or other confirmation of identity that is presented to verify that access to a resource is allowed.

"Device" refers to a networked device (e.g., workstation, laptop, smart phone, tablet, server, medical equipment).

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

"Workforce" means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health Sciences, is under the direct control of UCLA Health Sciences or the Regents of the University of California, whether or not UCLA Health Sciences pays them. The Workforce includes employees, faculty, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, house staff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health Sciences facilities from another institution.

POLICY

I. The only methods that may be used for remote access into UCLA Health Sciences networks are the

UCLA Health IT-supported remote access solutions that are listed in the Health Sciences Remote Access Standard. Any exceptions must have prior written approval from the Chief Information Security Officer. http://compliance.uclahealth.org/workfiles/HS%20Policies/InfoSecStandards/RemoteAccess.pdf

II. Remote access by Workforce members and other individuals

   A. Remote access may only be provided to individuals who have a UCLA Health Sciences business need for remote access.

   B. Workforce members must be authorized by their departments to use remote access.

   C. Departments may authorize remote access for non-workforce individuals such as Business Associates, vendor technical support, contractors, research collaborators and other third parties. (See HS Policy No. 9452, "*User Accounts; Passwords*," for information on establishing accounts for vendors, contractors and temporary staff.)

III. Remote access for external entities or groups of individuals

   A. When remote access is needed for external entities or groups of individuals, IT should be consulted on the appropriate remote access method as there may be more efficient and secure remote access solutions than setting up each individual with his or her own remote access.

   B. Such remote access connections for entities or groups must be approved in advance by the UCLA Health Sciences business owner and the Chief Compliance Security Officer or designee. Typical use cases would include, but are not limited to electronic interfaces, electronic data exchange, CareConnect server-side printing, vendor technical support and remote site connection.

   C. UCLA Health IT procedures for authorization, configuration and use must be followed.

   D. Remote access to UCLA Health Sciences electronic information resources must be limited to the minimum necessary to provide the required functionality.

   E. Any UCLA Health Sciences Restricted Information traveling across non-UCLA Health Sciences networks should be encrypted.

IV. Remote Access by Business Associates and other third parties

   A. Business Associates and other third parties must not remotely access Restricted Information until the appropriate Agreements are in place (HIPAA Business Associate Agreement when PHI is involved, the Data Security Appendix for Restricted Information that is not PHI).

   B. The business owner is responsible for establishing the rules for when Business Associates and other third parties may access their systems remotely.

      1. External technical support should never remotely access systems without prior approval of the system owner unless permission for this has been granted in advance.

      2. External technical support with permission to access systems without prior approval should keep an accurate log of who accessed which system for what and when.

V. Generic accounts must not be used for remote access. Any exceptions must have prior written approval from the Chief Information Security Officer.

VI. Any devices used to connect remotely to UCLA Health Science networks must comply with all applicable UCLA and UCLA Health Sciences policies. Requirements include, but are not limited to:

   A. Devices must run software for which critical security patches are made available in a timely fashion and must have all currently available security patches installed.

B. Current versions of anti-virus software must be running and the virus definitions must be kept up to date.

C. If there is a native host-based firewall, it must be enabled.

D. Mobile devices used by Workforce members for University Business must be encrypted.
For more information, see the following policies:

1. HS Policy No. 9421, *"Workforce Access to and use of PHI (Minimum Necessary)"*
2. HS Policy No. 9451, *"Use of Electronic Information"*
3. HS Policy No. 9453-C, *"Device and Removable Media Encryption"*
4. HS Policy No. 9457, "*Minimum Security Standards*"
5. UCLA Policy No. 401, *"Minimum Standards for Network Devices"*
6. UCLA Policy No. 404, *"Protection of Electronically Stored Personal Information"*

VII. Multifactor authentication should be used to secure both the remote access tools (such as VPN clients) and the systems being accessed remotely. (*see:* HS Standard 9452-B "*Health Sciences Multifactor Authentication Standard"*)

VIII. It is the responsibility of individuals who are allowed remote access to UCLA Health Sciences networks to ensure their remote access is never used to provide unauthorized access for others.

A. A UCLA Health Sciences computer account user must never provide his/her login password or other authentication credentials to others, including family members.

B. Authorized individuals connected remotely to UCLA Health Sciences networks must never allow others to use their remote access.

IX. Remote access may be monitored for malicious activity including but not limited to attacks on internal systems, network scanning, communications with known bad sites, malware, access from suspicious locations, etc. If there are any indications that the remote access is being used for malicious activities, the remote access may be disabled without prior warning.

X. Any additional eligibility or technical requirements of the Health Sciences Remote Access Standard must also be followed. See the Standard at the link below:
http://compliance.uclahealth.org/workfiles/HS%20Policies/InfoSecStandards/RemoteAccess.pdf

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

XII. Questions
Workforce members should consult their IT support group or the Office of Compliance Services - Information Security (CompOffice@mednet.ucla.edu) if they have any questions on this policy.

XIII. Exceptions to Policy
Unless an exception process is specified elsewhere in this policy, 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.

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 and 130203

University of California Business and Finance Bulletin IS-3, Electronic Information Security

University of California Electronic Communications Policy (ECP)

University of California Los Angeles, Policy No 401, Minimum Standards for Network Devices

University of California Los Angeles, Policy No. 404, Protection of Electronically Stored Personal Information

CONTACT

Chief Privacy Officer, Office of Compliance Services

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY (PRE-POLICYSTAT)

Approved:	February 22, 2006
Effective Date:	April 20, 2005
Review Date:	November 16, 2016
Revised Date:	November 2005; June 21, 2007; May 30, 2008, March 31, 2011, December 30, 2016

All revision dates:	07/2020, 12/2016, 03/2011, 05/2008, 06/2007, 11/2005

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval- President and CEO, UCLA Health	Johnese Spisso: Ceo Med Ctr [JB]	07/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	07/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	07/2020
Resnick Neuropsychiatric Medical Staff Executive Committee- Chief of Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	07/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	07/2020

Step Description	Approver	Date
Policy Owner	Liangzhou Chen: Mgr	06/2020