Effective Date:	*04/2005*
Approved Date:	*08/2020*
Revised Date:	*08/2020*
Next Review:	*08/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Use of Electronic Information by UCLA Health Workforce (Employees), HS 9451

PURPOSE

This policy sets forth guidelines for the use of Electronic Information Resources by the Workforce.

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:

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, or
    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 the 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" 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.

"Account" is an identity used to gain access to a particular computer, system or application.

"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.

"Authorized Personnel" means the ISS, DGIT, or Office of Compliance Services personnel designated to follow up on issues involving use of Electronic Information Resources.

"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.

"DGIT" is an abbreviation for David Geffen IT, the IT support group for the David Geffen School of Medicine.

"ISS" is an abbreviation for Information Services and Solutions. ISS provides central IT services, including networking, for UCLA Health in cooperation with DGIT and local departmental IT support groups.

"Password" is an authorized user's unique combination of numbers, letters, and/or symbols created by the user and used to securely access the UCLA Health Sciences computer, network or e-mail resources.

"Server" is a Device that provides some service for other Devices connected to it via the network. Servers may be physical or virtual.

"User" is anyone with access to UCLA Health Sciences Electronic Information Resources or Restricted Information.

"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, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health Sciences facilities from another institution.

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

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.

POLICY/PROCEDURE

I. **UCLA Health Sciences Electronic Information Resources may only be used for UCLA Health Sciences activities.**

   A. UCLA Health Sciences Electronic Information Resources are the property of UCLA Health Sciences and are to be used for the work-related business activities and operations of UCLA Health Sciences. These activities include communications with UCLA Health Sciences patients, clients, customers and Workforce in the normal course of business operations. Incidental personal use of UCLA Health Sciences Electronic Information Resources must comply with University of California policy. (*See: UC Electronic Communications Policy, Section III D.8.)*

   B. All data created using UCLA Health Sciences Electronic Information Resources shall remain the property of The Regents of the University of California.

   C. Any activity that is illegal under local, state, federal or international law, or disallowed by University of California, UCLA or UCLA Health Sciences policy is strictly prohibited, and may result in disciplinary action in accordance with HS Policy No. 9600, *"Responding to Compliance Issues"* and HS Policy No. 9461, *"Privacy and Information Security Sanction Policy."*

II. **General Requirements; Information for Users**

   A. All members of the UCLA Health Sciences Workforce must receive training on the Health Sciences Privacy and Information Security policies. (*See*: HS Policy No. 9460, "*Privacy and Information Security Workforce Training."*)

   B. Access to PHI and Restricted Information at UCLA Health Sciences is limited to those individuals for whom it is an authorized work-related requirement. (*See*: HS Policy No. 9421, *"Workforce (Including Employee) Access To and Use of Protected Health Information (PHI)"*; HS Policy No. 9452, *"User Accounts (Authorizing Access to Restricted Information; Passwords)."*)

   C. All members of the UCLA Health Sciences Workforce are responsible for ensuring compliance with the UCLA Health Sciences policies and safeguards to protect PHI, Restricted Information, and UCLA Health Sciences IT Resources including, but not limited to:

      1. accessing only the amount of PHI necessary to complete job responsibilities and **only** for those patients for whom the workforce member needs access to complete job responsibilities;
      2. securing the workstation or device on which PHI is being accessed when leaving the device for any reason; and
      3. logging out of computer applications when done with the job-related activity.

4. logging out from Single Sign-On solutions such as Okta when done with the job-related activity, especially on any shared, even temporarily shared, computers, and computers not issued and managed by UCLA IT.

D. Authorized users must use a sufficiently complex password to access systems containing Restricted Information. This password should be safeguarded from disclosure and must never be shared with any other person. Password requirements should be developed in accordance with the policies and procedures described in HS Policy No. 9452, *"User Accounts (Authorizing Access to Restricted Information; Passwords)."*

E. Every precaution should be taken to safeguard access to applications that contain confidential or Restricted Information.

F. All mobile devices and removable media used for University Business, including personally owned devices and removable media, must be encrypted and password protected consistent with HS Policy No. 9453-C, ***"Device and Removable Media Encryption."***

G. Restricted Information should either be:

1. stored on a UCLA Health Sciences IT managed network server;
2. de-identified (see: HS Policy No. 9440, ***"Release of Protected Health Information ("PHI") for Research Purposes"***);
3. removed from electronic data files; and/or
4. encrypted (*see*: UCLA Policy No. 404,*"Protection of Electronically Stored Information" and* the Office for Civil Rights "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."

H. All members of the UCLA Health Sciences Workforce should secure, maintain and when necessary, securely dispose of all removable electronic media that may contain Restricted Information according to established procedures. Removable electronic media includes, but is not limited to, portable hard drives, USB drives, flash memory cards, CD-ROMs, DVDs, and magnetic tapes. (*See*: HS Policy No. 9456, *"Physical Security of Restricted Information"* for more information on safeguarding and securely disposing of electronic media.)

I. Workforce members should use extreme caution when opening e-mail attachments received from unknown senders, because these may contain computer viruses and other malicious code. Workforce members should not click on links in emails from suspicious or unknown sources or provide personal account information or passwords in emails or on websites. Possibly malicious emails should be reported by forwarding them to DangerousEmail@mednet.ucla.edu and/or by using other UCLA Health Sciences-provided notification tools, if available.

J. Auditing, monitoring and investigations may be conducted as necessary by Authorized Personnel to ensure the security, privacy, integrity and availability of all UCLA Health Sciences Electronic Information Resources and compliance with all applicable UCLA Health Sciences policies.

1. The Chief Compliance Security Officer may initiate auditing, monitoring and investigations under this Policy at his/her discretion and the full cooperation of the individuals involved is required.
   a. All investigations related to unauthorized access or suspected breaches that are not already being handled by the Office of Compliance Services - Privacy must be reported to the Chief Compliance Security Officer.
   b. The Chief Compliance Security Officer and the Chief Privacy Officer may work jointly on

issues relating to auditing, monitoring and investigations.

c. The Chief Compliance Security Officer will escalate any issues as necessary to the Chief Compliance Officer, the Chief Information Officer and/or the Vice Chancellor, UCLA Health Sciences.

2. All such auditing, monitoring and investigations will be performed in compliance with the UC Electronic Communications Policy.
3. Access to equipment and system logs for auditing, monitoring and investigations must be granted to Authorized Personnel upon request. If necessary for an investigation, Authorized Personnel may take custody of equipment.
4. Any suspected or actual inappropriate access by a UCLA Health Sciences Workforce member may result in investigation and sanctions in accordance with applicable personnel policies.
5. Auditing, monitoring and investigations may include, but are not limited to the activities below:
   a. reviews of user and/or system access to any computing or communications device;
   b. reviews of user access to Institutional Information and IT Resources including reviews of audit trails;
   c. physical inspections of computer equipment, systems, devices, servers, printers, workstations and other devices;
   d. reviews of system configurations;
   e. monitoring of systems and network traffic for operational issues, malicious activity and use of Restricted Information; and
   f. interactive monitoring and logging of traffic on UCLA Health Sciences networks;
6. Network transmissions involving malicious activity or possible inappropriate disclosure of Restricted Information may be blocked.

K. The failure of any UCLA Health Sciences Workforce member to comply with UCLA Health Sciences Information Security policies, including any departmental security policies and/or procedures, may lead to disciplinary action in accordance with University personnel policies and collective bargaining agreements. Access to systems and applications may be suspended during the course of an investigation into alleged inappropriate use or access of UCLA Health Sciences Institutional Information. In all cases where an individual is placed on investigatory leave, access to systems and/or applications will be suspended at the time the individual is placed on investigatory leave.

L. All UCLA Health Sciences Workforce members must promptly notify the appropriate supervisory personnel and the Office of Compliance Services - Privacy and Information Security (CompOffice@mednet.ucla.edu) in the event of an actual or suspected privacy or information security incident. (*See*: HS Policy No. 9459, *"Privacy and Information Security Incident Reporting."*)

III. **Use of Restricted Information and Electronic Information Resources by UCLA Health Sciences Contractors and Suppliers**

No contractor or supplier doing business with UCLA Health Sciences shall be permitted access to UCLA Health Sciences Electronic Information Resources unless the contractor or supplier has first entered into a University-approved contract or agreement describing the services or supplies to be provided by the contractor or supplier and the security safeguards for the Electronic Information Resources and/or Restricted Information. In addition, a Business Associate Agreement executed in accordance with HS Policy No. 9430 *"Business Associates"* will be required if the supplier creates, receives, maintains or

transmits PHI. If the supplier creates, receives, maintains or creates non-PHI Restricted Information or has access to UCLA Health Sciences Information Resources, then the Appendix Data Security should be included in the contract. All such contractor and/or supplier access to Restricted Information shall have defined expiration dates.

Business and/or IT owners for suppliers or contractors working in their areas must immediately notify their IT support group to revoke access for any contractor or supplier staff member(s) who are no longer employed by the contractor or supplier as soon as they are aware that the individual(s) is no longer working for them.

IV. **Unacceptable Uses of Electronic Information Resources**

The following uses of Electronic Information Resources are examples of uses that are **prohibited** by UCLA Health Sciences policy, unless an exception is obtained as described below.

A. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and copyrighted music and movies.

The installation of any copyrighted software for which UCLA Health Sciences or the end user does not have an active license is strictly prohibited.

B. The exportation of software, technical information, encryption software or technology in violation of international or regional export control laws. Such activity is illegal and prohibited by UCLA Health Sciences policy.

C. The intentional introduction of malicious programs into the network or systems (e.g., viruses, malware, ransomware, etc.).

D. Revealing an individual-specific account password to others or allowing the use of an individual's account by others. This prohibition also prohibits an individual from sharing passwords with his or her family members or members of his or her household. Unauthorized access, release or dissemination of Restricted Information obtained by using a shared password may result in disciplinary action up to and including dismissal for the owner of the password.

E. Using a UCLA Health Sciences Electronic Information Resource to actively engage in procuring or transmitting material that is in violation of UCLA Health Science's sexual harassment policies and/or hostile workplace policies, including applicable laws and regulations.

F. Making fraudulent offers of products, items, or services originating from any UCLA Health Sciences account.

G. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

H. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorized to access, unless these duties are within the scope of regular duties. Network scanning may only be performed by Authorized Personnel.

I. Circumventing user authentication or security of any system, network or account.

J. Using any program/script/command or sending messages of any kind, with the intent to interfere with, or disable, network communications, via any means, locally or via the Internet/Intranet/Extranet, or initiating any denial of service attacks.

K. Providing any confidential information about UCLA Health Sciences workforce members to anyone,

including other UCLA Health Sciences workforce members, unless the provision of such information is part of the employee's job responsibilities and is authorized by the University policy.

L. Prohibited E-Mail and communication activities:

1. Sending any electronic communication that does not comply with the University of California "Electronic Communications Policy."
2. Sending any e-mail that contains Restricted Information that does not comply with HS Policy No. 9453-A, ***"Use of Electronic Mail (Email)."***
3. Sending unsolicited "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
4. Any form of harassment sent by e-mail, telephone or paging, whether through language, frequency or size of messages.
5. Unauthorized use or forging of e-mail header information.
6. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
7. Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
8. Posting the same or similar non-business-related messages to large numbers of recipients.

M. UCLA Health Sciences Restricted Information may not be posted to social networking sites or shared in other public forums without prior approval from the Chief Privacy Officer.

V. **Questions**

Should a workforce member have any question or concern about the appropriate security measures or use requirements, the workforce member should first discuss the issue with his or her supervisor. Supervisors and workforce members can contact the Office of Compliance Services - Privacy and Information Security (**CompOffice@mednet.ucla.edu**) with any questions regarding these security policies and procedures.

VI. **Enforcement**

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

VII. **Policy Exceptions**

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. Exceptions may be requested by submitting an exception request form.

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 1280.18

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. 404, Protection of Electronically Stored Information

University of California Los Angeles, Policy No. 420, Notification of Breaches of Computerized 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:	July 25, 2012, March 22, 2017
Revised Date:	November 2005; June 19, 2007; May 30, 2008, March 31, 2011, August 31, 2012, April 28, 2017

APPROVAL

Health Sciences Enterprise Compliance Oversight Board|

Approved 12/11/2010, 06/27/2012

All revision dates: 08/2020, 04/2017, 08/2012, 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]	08/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	08/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	08/2020
Resnick Neuropsychiatric Medical Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	08/2020

Step Description	Approver	Date
Executive Committee- Chief of Staff		
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	08/2020
Policy Owner	Liangzhou Chen: Mgr	07/2020