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*

User Accounts (Authorizing Access to Restricted Information; Passwords) Policy, HS 9452

PURPOSE

The purpose of this policy is to set forth the procedures by which authorized individuals shall be granted access to electronic Restricted Information and Electronic Information Resources to perform their job duties. This policy also sets forth the guidelines for managing individual user accounts in order to maintain the confidentiality, integrity and availability of Restricted Information as well as the requirements for individuals to safeguard their own authentication credentials.

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" 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.

"***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.

"*Multifactor Authentication*" requires a user to provide more than one kind of Authentication Credential to be allowed access to a system. In general, this would be at least two of the following: something you know (a password), something you hold (a secure token) and something you are (biometric identifier such as a fingerprint). Requiring at least two types of authentication provides protection if one credential is compromised.

"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, application, or other Electronic Information Resources.

"Unique User Identification" or "Unique User ID" is the unique identifier assigned to each individual authorized to access network, computer, and email resources containing Restricted Information for the purpose of identifying and tracking individual user identity to ensure access to Restricted Information is based on the individual's job responsibilities.

"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, house staff, 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.

POLICY

Individuals should only have access to UCLA Health Sciences Restricted Information and Electronic Information Resources as necessary for their job functions. UCLA Health Sciences shall determine which individuals are authorized to access Restricted Information and Electronic Information Resources in accordance with their job responsibilities. UCLA Health Sciences shall establish unique user identification for each individual who is authorized to access Restricted Information.

PROCEDURE

I. **Establishing User Accounts**

A. Access to UCLA Health Sciences Restricted Information and Electronic Information Resources is provided to individuals based on a job-related need for the access.

B. Each individual authorized to access Restricted Information will be assigned a unique User Identification or "User ID." The unique User ID will not be reassigned to any other staff member.

C. Access to UCLA Health Sciences Restricted Information and Electronic Information Resources is managed and authorized at the department level. The individual's supervisor is responsible to ensure that the individual has only the amount and extent of access required for their job duties. The supervisor should specify access for the individual to create, add, modify, delete, view and/or print Restricted Information. The supervisor will coordinate the assignment of the individual's User ID with the applicable system security department and/or System Administrator. The supervisor should monitor user access privileges on an ongoing basis and modify the privileges as the user's job function, role or responsibilities change.

D. For access to enterprise-wide Information Systems:

i. The supervisor will complete the online Access Request form specifying the access the new user will need to perform his/her job duties along with the individual's contact information and pre-defined authentication verifying information (e.g., mother's maiden name or other secret word).

ii. Access Request forms for non-employees must be submitted with the supervisor's signature and attached to the ServiceNow request.

iii. If access is being requested for a contractor or temporary Workforce member, an expiration date must also be specified on the authorization form. The expiration date may not exceed the term of the contract, length of assignment of the contractor staff in service to UCLA Health Sciences, or the period of temporary employment. In no event shall the expiration date be greater than one year from the authorization date, but may be renewed for an additional term. One week prior to the expiration date, ISS ID Management should request the supervisor to confirm whether the access is still required and provide an updated expiration date if needed.

iv. ISS ID Management will create a unique User ID for the individual, assign access as authorized by the department, and forward the User ID and the system-assigned password to the supervisor. ISS ID Management will not provide a User ID or system-assigned password until after verifying that the individual has completed any required Privacy and Information Security training.

v. The supervisor will provide the individual with his/her unique User ID. Upon logging in for the first time, the individual will be forced to change the system-assigned password to one known only to the individual.

E. For temporary access to clinical systems for registry or temporary staff, ISS ID Management will assign a unique User ID to the individuals after receiving a valid request from an authorizer such as Nursing Staff Officer. However, the Authorizer must request that the access be enabled each time the registry or temporary staff is called in to work. The access may only be enabled for the days of the work period and must be disabled no later than the end of the day on which the work period ends.

F. Supervisors will submit access requests as soon as possible to ensure the timely assignment of a unique User ID to all new UCLA Health Sciences Workforce members and other computer system users. ID administrators will maintain an emergency process to support the immediate need for assignment of unique User IDs, and for urgent changes to the extent of access of an individual User ID to Restricted Information.

G. Although the processes can vary for departmental and research systems, the supervisors and System Administrators for departmental and research systems are responsible to ensure that proper authorization, unique accounts and minimum necessary access to Restricted Information on those systems are in compliance with all UCLA Health Sciences and/or other applicable policies and procedures. In some areas, the supervisor will notify the System Administrator of the type and extent of access each individual should be granted. If end users make direct requests to System Administrators for access, the System Administrators are responsible for verifying the level of access and that the access is authorized with the supervisor or business owner of the application. Users may not be issued computer accounts for access to Protected Health Information until they have completed any required Privacy and Information Security training.

H. All authorization requests, whether for ISS or departmentally supported systems, must be documented and kept for 6 years after the first to occur of the following events: the user's access is terminated, the user is terminated, or the application/system is retired.

II. **Management of Accounts**

A. On a daily basis, the Human Resources Department will forward a list of employees who have resigned, retired, or otherwise terminated their employment with UCLA Health Sciences to ISS ID Management and Departmental IT support groups.

B. ISS ID Management and Departmental System Administrators will terminate all access to UCLA

Health Sciences systems containing Restricted Information immediately unless there are extenuating circumstances but in no case should access remain open for longer than 4 days after receiving the list.

C. Departmental Managers are responsible for **immediately** notifying ISS ID Management and Departmental System Administrators in the event an employee is terminated for cause, is provided an "Intent to Dismiss" letter, or is put on investigatory leave. ISS ID Management and Departmental System Administrators will immediately terminate all access to UCLA Health Sciences systems. Security codes that allow access to physical locations will be cancelled as well.

D. Departmental and Project Managers are responsible for notifying ISS ID Management and Departmental System Administrators when contractors or other non-Workforce members no longer require access to UCLA Health Sciences systems. In all cases of separation for cause, the notification should be immediate.

E. Managers, Directors and Supervisors are responsible for reviewing the access of individuals transferring in and out of their department to ensure that the individuals have only the access needed to complete their new job responsibilities. The Departmental Authorizer or Supervisor must notify ISS ID Management and local System Administrators of the access changes that need to be completed and the effective date of the changes. See Human Resource's Offboarding Separation/Transfer Guide.

F. Medical Staff Offices are responsible for notifying ISS ID Management in writing when a non-employed physician or other non-employed provider is no longer an active member of the medical staff.

G. Human Resources will provide ISS ID Management with a list of staff who are on extended sick leave or disability leave. The employee's access will be suspended until the employee is cleared to return to work. Supervisors and managers should notify ISS ID Management at least 2 working days prior to the employee's return to re-activate the employee's access. Departmental Human Resources will notify any local System Administrators of staff going on extended sick leave or disability leave. Any exceptions to allow computer access during leave must be approved by Human Resources.

H. Any accounts that have not been used for 90 days should be disabled. Users must contact the appropriate IT support group to have the account re-enabled. The IT support group must take appropriate measures to confirm that the individual is still entitled to access to the system or application in question.

I. On an annual basis ISS or the Departmental IT support will provide supervisors with lists of their employees and contractors who have access to applications containing Restricted Information to verify that user(s) still needs access. The manager will be responsible for verifying that the user(s) still needs access or should be removed within 10 business days of receiving the report. ISS or the Departmental IT support will be responsible for assuring that they receive the reports back and terminating any unnecessary access.
See HS Policy No. 9462, "*Privacy and Information Security Monitoring and Auditing*" for additional information on account monitoring.

III. **Assignment of Shared Logins**

Generic shared ID logins to systems that contain Restricted Information are prohibited unless an exception is approved in advance by the UCLA Health Sciences Chief Compliance Security Officer. Use of generic logins and passwords should be on a very limited basis. Approval may only be granted when patient care would be compromised by not using the generic login, or when such accounts are required

by vendor turn-key systems or applications. The password must be changed as soon as possible upon staff termination. These systems must be located in restricted access areas and the generic login shared on a strictly need-to-know basis.

IV. **System Administrator Account Management**

A. UCLA Health Sciences shall carefully manage system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum, provided only to personnel authorized to perform identified functions and allow the least privileges necessary to perform the required tasks. Passwords or other authentication measures should be changed upon the termination or change in job responsibilities of systems personnel who accessed these accounts.

B. UCLA Health Sciences should log activities performed by system administrator accounts and monitor logs on a regular basis.

C. Accounts for administrative access must comply with the requirements of the UCLA Health Sciences Administrative Access Standards which can be found at the link below: http://compliance.uclahealth.org/workfiles/HS%20Policies/InfoSecStandards/AdminAccess.pdf

V. **Passwords and other authentication credentials**

A. Passwords and/or other approved authentication credentials are required for all accounts used to access UCLA Health Sciences Restricted Information.

B. New users must change their passwords the first time they log in.

C. Vendor default passwords must be changed before systems go online.

D. Passwords should be considered "strong" based on the following criteria:

i. Passwords should be at least 8 characters long unless that computer system does not support 8 characters (in which case the password should be the maximum length and complexity of password characters supported by that system). Systems containing Restricted Information which cannot support a password length greater than 8 characters must request an exception.

ii. Where possible, passwords should contain characters from three of the following four categories:

i. English uppercase characters (A through Z)

ii. English lowercase characters (a through z)

iii. Base 10 digits (0 through 9)

iv. Non-alphanumeric characters

iii. Passwords should not contain User IDs or other context-specific information like the name of the system.

iv. Passwords should not be single words found in dictionaries for any language.

v. When a user creates a new password or changes an existing one, the password should be screened against lists of commonly used or compromised passwords and blocked if on those lists.

vi. Systems containing a password history function should implement that feature to prevent immediate re-use of the same password for up to five (5) passwords or the maximum the system supports.

vii. Users should not use the same password for different user accounts on the same system or across different systems.

E. Passwords must be temporarily locked out after no more than 10 invalid login attempts for all systems that can support a login lockout.

F. Passwords or other authentication credentials must not be shared. Any misuse of Information Resources or unauthorized access to Restricted Information using shared passwords or other authentication credentials will be treated as misuse by the authentication credential owner.

i. Passwords must not be kept in plain view, or stored in an easily accessible location.

ii. Authentication devices must be kept physically secure.

G. Mobile device users must not create passwords, passcodes or other authentication credentials on their devices that would allow access to Restricted Information by individuals (including, but not limited to, friends, family, students, and co-workers) who have no business need to access the Restricted Information. For example, you must not configure fingerprint access on your smartphone for others if that could allow them access to Restricted Information on your smartphone unless the access is necessary for their job duties. Any unauthorized access to Restricted Information using credentials configured on a device will be the responsibility of the owner of the device.

H. Systems should not store or transmit passwords in plaintext. Where possible, stored passwords should be encrypted using a salted hash or other suitable one-way encryption function. Files containing these hashed and encrypted passwords for use in authentication should be readable only with super user privileges.

I. If an individual has reason to believe that his or her password or other authentication credential has been compromised, the individual should report the compromise to the ISS Help Desk immediately so the standard Incident Response process can be followed. Any possibly compromised password should be reset as soon as possible.

J. Multifactor Authentication must be used as required by the Health Sciences Multifactor Authentication Standard, which can be found at the link below: http://compliance.uclahealth.org/workfiles/HS%20Policies/InfoSecStandards/MultifactorAuthentication.pdf

K. Customer support staff or System Administrators who have been asked to reset a user's lost password should take steps to verify that the identity of the person making the request matches that associated with the User ID being reset.

VI. Questions

Any questions on this policy should be referred to the Office of Compliance Services - Privacy and Information Security (**CompOffice@mednet.ucla.edu**).

VII. Enforcement

Any violation of this policy may result in disciplinary action up to and including termination of employment consistent with the University's personnel policies (see: HS Policy No. 9461, *"Privacy and Information Security Sanction"*). In some situations, it may be necessary to suspend user account privileges to prevent ongoing misuse while the matter is under investigation.

Offenses that are in violation of local, state and/or federal law will result in the immediate loss of computing privileges and will be reported to the appropriate University law enforcement authorities.

VIII. 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. The exception request form can be found at http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf

REFERENCES

FAQ on Authentication and Passwords can be found under Information Security at the link below:

http://compliance.uclahealth.org/body.cfm?id=189

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 Section 1280.15

National Institute of Standards and Technology Special Publication (SP) 800-63B, Authentication and Lifecycle Management

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 (PRE-POLICYSTAT)

Approved:	February 22, 2006
Effective Date:	April 20, 2005,
Review Date:	July 25, 2012. November 16, 2016
Revised Date:	November 2005; June 19, 2007, May 30, 2008, March 31, 2011 August 31, 2012, December 30, 2016

All revision dates: 07/2020, 12/2016, 08/2011, 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
Policy Owner	Liangzhou Chen: Mgr	06/2020