UC Riverside, School of Medicine Policies and Procedures
Policy Title: Access Control
Policy Number: 950-02-203

Responsible Officer:	Information Security Officer
Responsible Office:	UC Riverside School of Medicine (UCR SOM) Compliance Department
Origination Date:	06/27/2016
Date of Revision:	06/27/2016
Scope:	• All UCR SOM information, in an electronic format, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it. • All Technology Infrastructure owned and/or administered by UCR SOM • All UCR SOM divisions, including those of UCR SOM subsidiaries, if any • All UCR SOM workforce members, including employees, interns, contractors, consultants, and vendors doing business with UCR SOM including any individuals affiliated with third parties that access UCR SOM systems.

I. Policy Summary

The purpose of this policy is to define the process by which UCR SOM workforce members are granted access to UCR SOM computer systems including systems containing electronic Protected Health Information (ePHI) and other confidential information. The policy is also intended to describe the process for modifying or deactivating a workforce member's access to confidential data and ePHI as job responsibilities change, or as workforce members leave UCR SOM.

II. Definitions

Please refer to Standard Definitions Guide.

III. Policy Text

Access to electronic systems and ePHI is controlled by unique access codes (sign-on / user name) in combination with confidential passwords. Workforce members including employees, interns, contractors, consultants, and vendors will be assigned access to UCR SOM computer systems in accordance with their job responsibilities and job description on a need-to-know basis.

Each user who is provided access to electronic systems and ePHI is assigned an initial confidential password. Passwords are never to be shared with any other user.

The authority to request access and determine the appropriate level of access is the responsibility of the appropriate department head.

IV. Responsibilities

All UCR SOM computing users.

V. Procedures

A. Confidentiality Statement

To obtain access to UCR SOM electronic systems, all workforce members must read and agree to the UCR SOM Code of Conduct provided through the Learning Management System (LMS).

B. Role Based Access

System access will be granted based on the workforce member's (user) role within the organization. The workforce member will have access to all of the information they need to perform their job functions, conduct UCR SOM business and/or care for patients, but not more than they require for these purposes. Access will be granted upon completion of applicable training.

Access roles will be reviewed and modified, if needed, when a workforce member changes job responsibilities within the organization. The department accepting the transferred workforce member from the originating department is responsible for ensuring that employee's access is appropriate to their new role. It is crucial to ensure the termination of user access to information systems or functions that are no longer needed upon transfer for the workforce member.

C. Access to Privileged Accounts

A background check must be completed for UCR SOM staff with access to privileged accounts, such as System Administrators, Security Administrators, or Electronic Medical Record System Administrators, prior to being granted access to the accounts.

D. Access Termination

Access to the UCR SOM Network Identification (Net ID) and any accounts granting access to systems containing ePHI or confidential data is terminated within 5 working days from the date of separation. Access to the individual department electronic systems not using the UCR SOM Net ID will be terminated as soon as possible when a workforce member leaves UCR SOM but not more than 30 days from the termination date.

E. Limited Time Access

Workforce members, contractors, temporary employees, or other guests who will be at the University for a defined or limited period of time will be granted access to the applicable systems and information with a defined start and end date to ensure that access is deactivated after the end of the time period.

The department manager is responsible to ensure that the access for individuals requiring access on a limited basis is terminated at the point that the contract or temporary assignment is ended. The manager will serve as the designated host for requesting the sponsored account.

F. Access Request

The UCR SOM Net ID is granted to each member of the faculty, staff, and student population at UCR SOM. For the duration of the relationship with UCR SOM, these individuals will use the individual UCR SOM Net ID to access general online services. The UCR SOM Net ID is provisioned by UCR SOM Office of Information Technology (OIT).

Requesting UCR SOM network access and obtaining assistance with the UCR SOM Net ID may be obtained through UCR SOM OIT.

Access to UCR SOM Electronic Medical Record (EMR) systems is granted to each workforce member that requires access to clinical information systems. Requesting access to the UCR SOM EMR system is done through the OIT in the form of an access request ticket.

G. Access to Department-Specific Systems

Provision of access for workforce members to department-specific electronic information systems, such as department network shares, will be requested through UCR SOM OIT in the form of an access request ticket.

H. System Access Compliance and Regulation

Data utilized in business operations is considered an asset of the University. All employees are accountable for the protection of this data from intentional or accidental unauthorized access, modification, destruction, or disclosure.

Patients understand that services provided by UCR Health are private and confidential, and that to enable UCR Health to perform those services, patients furnish information with the understanding that it will be kept confidential and used only by authorized persons as necessary in providing these services. It is also recognized that the good will of UCR Health depends on keeping services and information confidential, and that certain legal obligations attach to this information.

Failure to comply with the UCR SOM electronic information security policies constitutes improper conduct. Improper conduct, includes but is not limited to the following:

- Disclosure of a password.
- Attempting to gain or use a sign-on code or password that belongs to another person.
- Attempting to gain access to electronic systems for purposes other than official business. This would include completing fraudulent documentation to gain access.
- Using an authorized password to invade patient privacy by examining records or data for which there has been no request or need for review.
- Loading or use of unlicensed or non-approved programs or games.
- The use of unlicensed or non-approved software constitutes a serious risk to medical operations. Staff who use software not properly licensed or approved will be subject to disciplinary action.
- Unauthorized disclosure of confidential information.
- The intentional unauthorized destruction of University data.

UCR SOM OIT terminates temporary and emergency accounts based on a predetermined time established at account activation.

UCR SOM OIT can elect to automatically inactivate accounts after 6 months of inactivity.

UCR SOM OIT employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

UCR SOM OIT restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

I. System Timeout / Automatic Log-Off:

Automatic session log-off to UCR SOM network is initiated after a predetermined period of inactivity (timeout period). The session log-off remains in effect until the user reestablishes access using the appropriate identification and authentication procedures. The predetermined period of inactivity on the workstations ranges from 5-20 minutes. The timeout period setting for various enterprise workstations is risk based related to workstation accessibility.

UCR SOM OIT enforces a limit of 5 consecutive invalid UCR SOM Net ID access attempts by a user during a 30-minute time period. UCR SOM OIT automatically locks the account for 30-minutes when the maximum number of unsuccessful attempts is exceeded.

VI. Forms/Attachments Not Applicable

VII. Related Information Not Applicable

VIII. Revision History

New 6/2016

Approval(s):

Compliance Committee (07/19/2016)