UC Riverside, School of Medicine Policies and Procedures
Policy Title: Privacy and Security Site Review
Policy Number: 950-02-012

Responsible Officer:	Chief Compliance & Privacy Officer
Responsible Office:	Compliance and Privacy
Origination Date:	05/2016
Date of Revision:	08/2024
Scope:	UC Riverside School of Medicine/ UCR Health

I. Policy Summary

State and federal law impose particular standards for health care organizations to protect the privacy and security of protected health information (PHI) and electronic protected health information (ePHI). This policy describes how UCR Health ensures complies with organizational privacy practices undertaking periodic assessments of the physical environments where PHI and ePhi are used and stored in order to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of such PHI and ePhi.

II. Definitions

For definitions in this policy, refer to the HIPAA privacy and security implementing regulations at 45 CFR Parts 160, 162, and 164.

III. Policy Text

The Compliance Advisory Services Department will perform periodic privacy and security walk-throughs to ensure employees are following all UCR Health's privacy and security policies.

IV. Responsibilities

Compliance Advisory Services

V. Procedures

A. A walk-through of a rotating sample of UCR Health clinics and and other UCR School Of Medicine locations where PHI/ePHI may be housed will be performed from time to time and will be coordinated through Compliance Advisory Services.

B. A Privacy and Security Walk-Through Checklist, (Attachment A) that compares security requirements with actual employee practices, will be completed for each walk-through visit. The Checklist may be updated from time to time based upon regulatory changes and organizational priorities.

C. Areas to be reviewed will include:

1. Employee Conduct
2. Workstation Use
3. Access Control
4. Environmental Control

D. When a privacy and security standard is not met, staff will be given immediate in-service training which will indicate the area of deficiency and the standard which must be met. This in-service training will be documented on the Privacy and Security In-Service Form (Attachment B). Other corrective actions also may be implemented, depending upon the finding.

E. Potential privacy breaches will be investigated and any verified privacy breach will be reported pursuant to School of Medicine policy.

VI. Forms/Instructions

Attachment A: Privacy and Security Walk-Through Checklist
Attachment B: Privacy and Security In-Service Form

Approvals:

COMPLIANCE COMMITTEE (09/03/2024)

Signed by:
Paul Hackman
BC5CF44DC0494EA...

9/20/2024 | 10:59 PM PDT

PAUL HACKMAN, J.D., L.LM.
CHIEF COMPLIANCE AND PRIVACY OFFICER,
SCHOOL OF MEDICINE

DATE

Signed by:
Deborah Deas
870C12B416E84CB...

9/21/2024 | 4:45 PM PDT

DEBORAH DEAS, M.D., M.P.H
VICE CHANCELLOR, HEALTH SCIENCES
DEAN, SCHOOL OF MEDICINE

DATE

UCR HEALTH

Attachment A

Privacy and Security Walk-Through Checklist

Practice Site: _____ **Date:** _____

Employee Conduct	Yes	No	Comments
Employees and visitors wear ID badges			
Employee challenge persons who are not wearing badges			
Employees protect PHI by speaking softly and, when appropriate, using nonpublic areas			
Workstation Use	**Yes**	**No**	**Comments**
Workstations and computer monitors are positioned to prevent unauthorized persons from viewing EPHI or privacy screens are in place			
Employees protect user IDs and passwords and don't share them			
Employees don't share workstations while logged in			
User IDs and passwords are not posted on or near workstations			
Documents with PHI are Face Down or concealed, especially in public areas and when employees leave their workstations			
When documents with PHI are not in use, they are stored or filed so as to avoid observation or access by unauthorized persons			
Unattended computers are returned to the logon screen or have password-enabled screen savers when not in use			
All computers are logged off after hours			
Laptops, PDAs and other portable equipment are physically secured with lock that does not have a key present or nearby			
PHI on printers, photocopiers or fax machines is always attended by employees			
Backups of EPHI are secured in a safe area (off-site and not in or near workstation			
PHI is shredded or discarded in secure container and not in regular trash.			
Access Control	**Yes**	**No**	**Comments**
Doors with access-control mechanisms, such as locks or swipe- cards systems are closed			
Access to computer room is restricted to authorized personnel			
Access to printers and FAX machines is limited to authorized staff			
Office doors, filing cabinets and desks are closed and locked when unoccupied			
Office doors, filing cabinets and desks are locked and building is properly alarmed after hours			
Environmental Controls	**Yes**	**No**	**Comments**
Smoke detectors and fire extinguishers are accessible and operational			
Computer equipment is plugged into surge protectors and, where appropriate, uninterruptible power supplies			

Attachment B

Privacy and Security Audit In-service

Practice Site: _____ **Date:** _____

Area of Deficiency: _____

Standard to be met: _____

In-service Education Provided by: _____

Name: _____ Title: _____

Staff in attendance:

Name: _____ Title: _____

Name: _____ Title: _____

Name: _____ Title: _____

Name: _____ Title: _____