UC Riverside, School of Medicine Policies and Procedures
Policy Title: 950-02-202 - Information Security Management
Policy Number: 950-02-202

Responsible Officer:	Information Security Officer
Responsible Office:	Compliance Advisory Services
Origination Date:	03/10/2016
Date of Revision:	09/28/2016
Review Date:	09/03/2024
Scope:	▪ All UCR School of Medicine (SOM) information, in its electronic form, 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 Health subsidiaries, if any; ▪ All UCR SOM facilities, including those of UCR SOM subsidiaries, if any; and ▪ 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. This policy addresses security management for all types of sensitive data and systems including research and financial data.

I. Policy Summary

The purpose of this policy is to establish methods for safeguarding the confidentiality, integrity, and availability of all sensitive information throughout its lifecycle. Sensitive information includes electronic protected health information (ePHI), payment card data, personnel data for employees and other members of the workforce, and any other sensitive information as defined by the UCR SOM.

This policy defines UCR SOM's security management framework and establishes a formal risk management program by assigning responsibility for risk identification, analysis, mitigation, and program management. Responsibility for program management and oversight includes the active involvement of executive leadership, departmental management, data stewards, and others with information management responsibility.

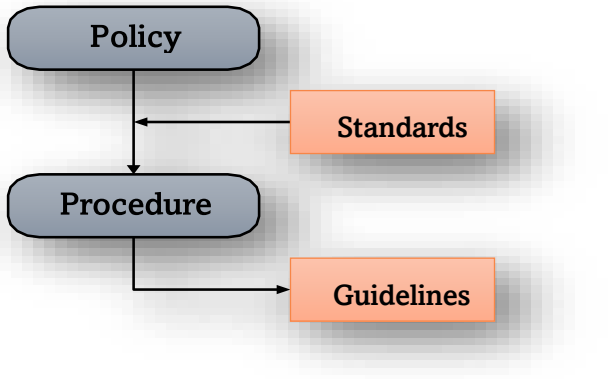
The goal of the UCR SOM security management program is to protect the confidentiality, integrity, and availability of sensitive information by allocating resources commensurate to the risks identified through the risk assessment process. In addition, the security management program will provide the governance structure and resources to meet the University of California and UCR SOM's legal, regulatory, and contractual requirements.

Any breaches of information security, actual or suspected, will be reported to, and investigated by the designated Information Privacy & Security functions of UCR SOM.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires all covered entities, including UCR SOM, to implement privacy and security safeguards to protect the confidentiality, integrity, and availability of protected health information. In response, the Department of Health and Human Services published a series of rules, including the HIPAA Security Rule, which contain standards and implementation specifications required to achieve this goal. The rule also requires covered entities to

conduct risk assessments to document the probability and potential consequence of adverse events, and then implement controls to lower the risk.

This policy acknowledges the hierarchy of governance, and augments security laws and policies issued by the State of California, the University of California Office of the President (UCOP), and related policies published by the University of California, Riverside. This policy may be supplemented with additional policies or procedures for subsets of UCR SOM, or user groups supported by UCR SOM, providing the governance is more restrictive.



This security policy represents the foundation layer of UCR SOM's policy framework and complies with the objectives set by the legal and privacy regulations. It also provides a foundation for various Information Security procedures, standards, and guidelines.

In the event of a conflict between this document and laws or policies issued by higher levels of authority, the more stringent regulation or document shall be followed.

It is the policy of UCR SOM to implement appropriate information security controls to protect the confidentiality, integrity, and availability of sensitive information.

II. Policy Text

UCR SOM will:

- **A.** Maintain a governance structure to manage information security through the application of sound security management principles
- **B.** Defend against unauthorized access through the implementation of security controls
- **C.** Evaluate the effectiveness of the implemented controls through periodic and continuous monitoring
- **D.** Adjust existing and/or add new controls, as needed, to respond to a changing risk environment
- **E.** Detect, using reasonable means, attempts by persons or systems to gain unauthorized access to sensitive data or computing resources
- **F.** Grant, modify, or remove access to information and systems based on a validated need to know through the use of formal documented and auditable processes and procedures
- **G.** Deter unauthorized access by members of the workforce through user education, random and event-driven auditing, and tiered sanctions to those who violate policies
- **H.** Hold individuals accountable for their actions misusing sensitive information and information systems
- **I.** Ensure patient confidentiality by limiting use and disclosure of PHI to the minimum necessary for the purpose of the use or disclosure
- **J.** Adopt a formal process to respond to security incidents to meet applicable law, regulation, and contractual requirements in order to minimize the negative impact to patients, staff, or the University
- **K.** Provide for the timely recovery of information and back up processing in the event of lost information or system capabilities
- **L.** Establish a formal program to protect the physical and electronic environment, as well as the supporting infrastructure where sensitive data resides, from unauthorized individuals
- **M.** Define the appropriate use of information systems in support of the business purpose
- **N.** Limit access to devices that contain sensitive information and properly wipe and dispose of those devices when no longer needed

O. Hold those third parties who have a validated need to access sensitive data, accountable to the highest level of information assurance required by law, regulation, or contract
P. Preserve the integrity of sensitive data through the implementation of operational controls that protect the computing environment
Q. Preserve UCR SOM's ability to meet the legal, regulatory, and contractual requirements

III. Responsibilities

A. Senior Management Team

The Dean of the SOM, CEO, and CIO comprise the senior management team and have the following roles and responsibilities:

1. Establish and sustain an enterprise-wide information security program with adequate resources to address perceived risks
2. Provide executive direction and support for the enterprise information security goals and objectives
3. Set the organization's cultural and managerial tone for risk management, compliance, and security through top-level policies
4. Appoint personnel to oversee the information security program

B. Compliance Committee

The SOM Compliance Committee shall oversee HIPAA privacy and security. The Compliance Committee is composed of representatives and designees from UCR campus and the SOM, including UCR Health.

The Compliance Committee has the following roles and responsibilities specific to information security:

1. Provide interdisciplinary input and guidance for the development and maintenance of information security management policies, procedures, standards and guidelines
2. Provide oversight to assure that the information security management plan is compliant with applicable Federal, state and local laws/regulations, contractual obligations, and University policy
3. Serve as members of the security incident response team to address the regulatory breach reporting requirements as needed
4. Provide cross-departmental input and support to ensure workforce members receive appropriate information security awareness training
5. Examine potential and/or actual areas of non-conformance and recommend, develop and ensure corrective action or sanctions

C. Information Security Officer (ISO)/HIPAA Security Officer

The ISO is designated by UCR SOM as the senior security official as defined in 45 CFR §164.308(2) and has the following roles and responsibilities:

1. Develop and implement the policies and procedures required to achieve compliance with the HIPAA Security Rule for the covered entity
2. Direct and update the HIPAA Security Compliance Program to assure compliance with current HIPAA Security regulations
3. Oversee security risk assessment of the UCR Health clinical information systems, and implements an effective Risk Management Plan to minimize risks to the confidentiality, integrity, and availability of ePHI
4. Coordinate audits of UCR SOM information systems to ensure compliance with information security requirements and policies
5. Provide education and training to UCR SOM workforce members on HIPAA security policies and procedures

6. Develop and assist in the implementation and maintenance of UCR SOM information security policies and procedures in coordination with the compliance and privacy officer, the chief information officer, and legal counsel
7. Provide technical vision and leadership in support of the continued development of UCR SOM security architecture
8. Develop and maintain information security management policies, procedures, standards and guidelines
9. Review the results of risk assessments and make adjustments to the security management program, as appropriate
10. Participate in the development of the annual information security review and work plan
11. Direct all network security tasks and assessments
12. Provide information security management oversight, assuring compliance with the HIPAA Security Rule
13. Develop and implement procedures for detecting, reporting, and responding to security incidents
14. Oversee the risk assessment process and provide assessment reports
15. Ensure that workforce members receive appropriate information security awareness training

IV. Procedures

A. Information Security Risk Assessment

1. Risk Assessment Objectives

   The primary objective of the HIPAA Information Security Assessment is to evaluate and identify potential threats and vulnerabilities to the security of the confidential information in the custody of the UCR SOM. This assessment will help in the creation of a plan to reduce and mitigate risks that might negatively impact the confidentiality, integrity, and availability of this information. Information security risk management is not a one-time event, but an ongoing venture that follows a cyclical process.

   a. *External Risk Assessment:*

   UCR SOM participates in a risk assessment of its Information Technology general controls (ITGC) performed by an external auditor.

   b. *Information System Security Assessments:*

   UCR SOM shall conduct an Information System Security Assessment to identify the electronic information resources that require protection, and to document risks from potential threats or vulnerabilities to electronic resources that may cause loss of confidentiality, integrity, or availability of ePHI. Such risk assessments will take into account the potential adverse impact on the University's operations, assets, and reputation. The Information System Security Assessment will be utilized to develop and maintain a Security Risk Management Plan to identify and reduce ongoing and potential risks.

   c. *Periodic Risk Evaluation*

   This periodic assessment serves to evaluate the overall IT infrastructure organization, including network flow architecture, system integration, and security program administration.

   A security work plan is developed based on this assessment and approved by administration for implementation support.

2. Risk Management

   Security measures and controls to sufficiently reduce risks and vulnerabilities, as identified in the risk assessment, will be implemented.

3. Information System Activity Review

   Regular review of information system activity, such as audit logs, access reports, and security incident tracking reports will be performed.

   Documenting incidents, implementing remediation strategies, reporting to management, and complying with legally mandated notification requirements will be performed by the Compliance Office.

4. Sanctions

   Appropriate sanctions will be taken against workforce members who fail to comply with UCR SOM's privacy and security policies and procedures. (See UCR SOM Policy Privacy & Security Sanctions Policy for details).

5. Assigned Security Responsibility

   The ISO shall coordinate the implementation of the safeguards required under this policy, including the development and implementation of information security policies and procedures.

6. Workforce Security

   Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as described under HIPAA's Information Access Management standard, and to prevent unauthorized access.

7. User Authorization and/or Supervision

   Workforce members are assigned appropriate authorization to work with ePHI as needed to perform their assigned job duties. System access authorization is described below in the Access Authorization, Establishment and Modification section.

8. Workforce Clearance

   All clinical workforce members are required to pass screenings and successfully complete a criminal background check prior to employment. Individual system data stewards determine and provide workforce member access to ePHI as appropriate to the scope of each member's assigned duties and responsibilities.

9. Termination Procedures

   A separation/termination process is managed by UCR SOM Human Resources when a workforce member's employment ends. This process includes a Helpdesk ticket requesting de-activation of system accounts and equipment retrieval. UCR SOM network account access is also deactivated through this process.

10. Access Authorization, Establishment and Modification

    Access to computers containing ePHI is controlled by confidential access codes and unique passwords. Authority to determine access levels for staff and faculty is the responsibility of the appropriate director, department head or data steward and is granted according to need.

    User access code requests must be submitted in writing using the Helpdesk ticketing system. The request is completed by the appropriate Supervisor, Coordinator, Department Head or Director. Authority to request codes can be delegated to identified users/training coordinators.

    System Data Stewards modify the user's right of access to ePHI as appropriate to the scope of the member's assigned duties and responsibilities.

11. Malicious Software Protection

    All computers that connect to the UCR SOM IT infrastructure, including all off- campus computers that connect remotely (e.g., via wireless or VPN) will be protected with UCR SOM approved anti-

virus/anti-malware software. All anti- virus/anti-malware software will conform to UCR SOM software standards and will have up-to-date virus definitions. This policy applies to all desktop and laptop computers, regardless of ownership or location.

12. Anti-Virus/Anti-Malware

    Software will be installed in such a manner that all settings are password protected and may not be altered in any way which would reduce the effectiveness of the software.

    Each deployment of anti-virus/anti-malware software will be configured to ensure timely automatic updates of virus definitions.

13. Access Monitoring

    Each information system generates log files of system activity which identify individuals who have accessed ePHI. Evaluation of these log files is performed to determine if inappropriate access to ePHI has occurred. Inappropriate access includes any access not necessary for the workforce member job duties at UCR SOM.

14. Password Management

    Electronic systems containing restricted information must be password protected to control access to restricted information. Password protected access maintains the confidentiality and integrity of electronic data and protects the University's computing resources and infrastructure. The UCR SOM Password Security policy establishes a minimum standard for the creation of strong passwords, the protection of those passwords, and frequency of password changes.

B. Information Security Incident Response

1. Information Security Incident

   An information security incident is a violation or imminent threat of violation of computer security policies, information security safeguards, acceptable use policies, or standard security practices that impact the confidentiality, integrity, and availability of health information.

   Examples of information security incidents include but are not limited to the following:

   - Transmission of an email or fax to the wrong recipient
   - Unauthorized access of patient information
   - Unauthorized disclosure of patient information
   - Electronic media such as a laptop, CD, portable devices, computer hard drive, or other similar equipment is stolen or missing and contains unencrypted personally identifiable information.
   - Unauthorized access to University servers or devices by external sources (hacking).
   - Computer security intrusion
   - Unauthorized use of systems or data
   - Unauthorized change to computer or software
   - Loss or theft of equipment used to store private or potentially sensitive information
   - Denial of service attack
   - Interference with the intended use of information technology resource
   - Compromised user account

2. Information Security Incident Reporting Responsibilities and Methods

   If a UCR SOM workforce member discovers that there has been an Information Security incident or suspects that an incident or breach has occurred, they must immediately report the incident to their immediate supervisor.

3. In the event of a potential breach, refer to Policy *950-02-225 - Privacy & Security Breach Response & Incident Notification Plan*

4. Post-Incident review and corrective action
    a. The Incident Report will be reviewed, as needed, by the compliance and privacy officer, legal counsel, and risk management
    b. Interference with the intended use of information technology resource's, such as a computer security intrusion, will be immediately referred to and addressed by UCR SOM IT staff to implement corrective action
    c. A determination will be made as to which, if any, of the notification requirements have been triggered under both state and federal law. The applicable notices will be made to the affected individuals and to the applicable state and federal authorities, and through media outlets as required under federal law
    d. Use of the information gathered through the Incident Report process is reviewed, trended and utilized to develop corrective or process improvement plans. Those plans are then implemented, as appropriate, evaluated on an ongoing basis, and reported to the SOM Compliance Committee
5. Contingency Plan

    The University has made provision for responding to an emergency or other occurrence (e.g. fire, vandalism, system failure, and natural disaster) that damages systems containing ePHI.
6. Data Backup Plan (Required)

    Backing up digital communications, data, and other electronic files is an essential practice to prevent the loss of valuable information. The purpose of performing backups is to be able to restore a system to a known state (as of the date of the most recent back-up) in case of system failure or a catastrophic data loss event.

    All ePHI data hosted in the UCR SOM Data Center, unless otherwise requested will include, at a minimum, backup (duplicate) copies of the data. These copies are stored in a protected and secure location and moved to an off-site storage location within one month of creation. The backup process uses either data copied to tapes or replicated to an alternate storage area network (SAN). In both cases, the data is transferred and housed at an off-site secure facility.

    Documentation that indexes the data backups and their storage locations is maintained by UCR SOM IT. This information is also maintained and kept with the storage systems and the data. This provides a means to identify and retrieve the appropriate data in the event that on-site documentation is destroyed.

    For example, backup tapes that are sent to an off-site vendor (i.e. Iron Mountain) are recorded in the backup server's media database. Hardcopy data indexes are also stored with the backup tapes.

    In the event of a disaster resulting in the loss of the primary data stored at UCR SOM, data recovery is accomplished by retrieval from off-site storage.

    Protocols documenting system recovery using the retrieved backup media is maintained by UCR SOM IT.

    Periodic testing of data recovery from backup media is conducted and documented by UCR SOM IT. This may also include actual recovery events.
7. Disaster Recovery Plan (Required)

    Restoration of system availability and data recovery are crucial for ensuring continuity of business and patient care operations and the safety of staff and patients.

    Details of the Disaster Recovery process is provided in the Disaster Recovery and Contingency policy.

8. Emergency Mode Operation Plan (Required)

   During an interruption of electronic information services, either by forces of nature or system failures, provision of critical patient care and business functions including the availability of a complete medical record, will continue by implementing an Emergency Mode Operation Plan, also referred to as "Computer Downtime" mode.

   If the interruption of electronic services is a result of an internal or external disaster, the UCR SOM Incident Command System (ICS) may be instituted. This system provides for a command structure and processes to ensure continuation of operations.

   When there is a loss of electronic facility access control, staff will provide manual access provisioning and added property surveillance to guard against unauthorized physical access to PHI.

9. Testing and Revision Procedures (Addressable)

   (See Computer Downtime: Backup and Recovery policy for details regarding periodic testing and revision of contingency plans.)

10. Applications and Data Criticality Analysis (Addressable)

    Assessment of the relative criticality of applications and data is obtained and documented by UCR SOM IT. Criticality levels include Mission Critical, Patient Care and Standard designation. This designation is recorded in the UCR SOM IT application inventory database.

11. Standard: Evaluation (Required)

    Periodic technical and nontechnical evaluations are performed, initially based upon the standards implemented under this rule, and subsequently in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirements of HIPAA subpart 164.308(a)(8).

12. Information Security Risk Analysis

    Periodic risk evaluation of UCR SOM core computing infrastructure and security administration.

13. Physical Safeguards

    a. *Standard: Facility Access Controls*
       The following standards are implemented to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

    b. *Contingency Operations*
       Procedures that allow facility access in support of restoration of lost data under the Disaster Recovery Plan and emergency mode operations plan in the event of an emergency are governed by the Incident Command System (ICS).

    c. *Facility Security Plan*
       Facilities and the equipment therein are safeguarded from unauthorized physical access, tampering, and theft.

       Centralized computer facilities that house core data are protected in a secure location with physical access controlled by UCR SOM IT Department.

       Computer facilities that process departmental data may require physical security depending on the value and sensitivity of the data they process, the resources they access, and their cost. Examples of facility physical safeguard security would include locating data storage behind locked doors, limiting access to a building via a controlled reception desk, video

surveillance of building access point among others. Physical security management of these departmental resources is the responsibility of the department.

d. *Access Control and Validation Procedures*
The following policies are implemented to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

UCR SOM workforce members must carry and display UCR SOM identification badge in accordance with procedures established by UCR SOM Human Resources. Building access is controlled and restricted by the use of keyless electronic locks activated by the badges where applicable.

Visitor and vendor physical access is controlled at entrance points with the use of staffed reception areas. All visitors must sign in to a visitor log and receive a visitor badge. The visitor badge identifies that this person is restricted from all areas where they could gain access to protected information. All staff is trained to be on guard to ensure that visitors are permitted only in non-restricted areas.

Vendors requiring access to software or hardware for maintenance or troubleshooting will be escorted and overseen by UCR SOM workforce members.

e. *Maintenance Records*
   i. UCR clinics will keep a record of all repairs and modifications to the physical components of the facility that are related to security (for example, hardware, doors, walls, and locks).
   ii. This documentation is maintained for 7 years.
   iii. IT Asset Management system is used to track and record maintenance documentation performed on Health Care electronic information resources.

f. *Workstation Security*
Reasonable physical safeguards will be maintained for all workstations that access ePHI, to restrict access to authorized users. If workstations must be left in areas unattended by staff that area must be locked to restrict access from non- UCR staff.

The following are minimum requirements for workstation security:

Time-out - Workstations will be configured so that after a period of inactivity, the workstation will automatically log-off requiring the user to log in again to utilize the workstation.
Local storage of restricted information on workstation hard drives is prohibited.
Device and Media Controls - The receipt, utilization and removal of workstations, hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility are governed by the following requirements:
Only University issued or UCR SOM IT approved computer or mobile devices are permitted to access the UCR SOM Network.
All UCR SOM issued computers or portable computing and electronic storage devices must be returned to UCR SOM when the workforce member leaves the University.
Media Disposal - In the event any workstation or computing device containing ePHI is not to be reused, the media must be sanitized as per industry standards prior to disposal. The allowable method for media sanitization is described as per University policy. (See Media Usage, Re-Use & Destruction policy).
Media Re-Use - In the event any workstation or computing device containing ePHI will be reused the media must be sanitized prior to reuse of that media. The allowable method for media sanitization is described as per University policy. (See UCR SOM policy "Media Usage, Re-Use & Destruction").

Accountability UCR SOM IT support staff will document and maintain a record of the movements of hardware and electronic media. This record is maintained in the asset management system and will include the name of the users and UCR SOM IT technical staff associated with each relocation.

Data Backup and Storage - When possible, files containing restricted information must be stored on network shared drives secured by UCR SOM IT rather than locally on devices. Storage of electronic files containing unencrypted restricted information on local device drives is not permitted.

If local storage of restricted information cannot be technically avoided, a retrievable, exact copy of the information, when needed, should be captured before movement of equipment.

C. Security Awareness and Training

1. Formal Security Training

   The University has implemented a plan of information security education throughout the institution that will promote an on-going understanding about information security risks and recommended practices.

   UCR SOM has a multi-pronged approach to training and awareness. Current strategies include:

   a. An overview of information security awareness is part of new hire onboarding. Continuing education on information security is included as part of the required annual training program for each workforce member.
   b. An information security website that serves as a common repository of information security educational materials, current issues, policies and practices.

2. Security Reminders

   Periodic communiqués are provided to the University community alerting UCR SOM personnel to specific vulnerabilities. These come in the form of emails via “Privacy and Security Reminder” or on an as needed basis.

V. Related Information

COPPA Children’s Online Privacy Protection Rule
http://www.ftc.gov/coppa/
DMCA Digital Millennium Copyright Act
http://www.copyright.gov/legislation/dmca.pdf
ECPA Electronic Communications Privacy Act
http://www.access.gpo.gov/uscode/title18/parti_chapter119_.html
FERPA Family Educational Rights and Privacy Act
http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
GLBA Gramm-Leach-Bliley Act
http://www.ftc.gov/privacy/glbact/
HIPAA Health Insurance Portability and Accountability Act
http://www.hhs.gov/ocr/hipaa/
Patriot Act
http://www.fincen.gov/statutes_regs/patriot/

VI. Revision History

Origination Date: March 2016
Revision Date: September 2016
Review Date ***(Reviewed by CCM with no revisions)***:
September 2024

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