UC Riverside, School of Medicine Policies and Procedures Policy
Title: Access to Electronic Medical Record
Policy Number: 950-02-002

Responsible Officer:	Compliance and Privacy Officer
Responsible Office:	Compliance and Privacy Office
Origination Date:	3/2016
Date of Revision:	
Scope:	SOM and all UCR Health Faculty Practice Locations

I. Policy Summary

This policy covers all electronic protected health information (ePHI), which is a person's identifiable health information. This policy covers all electronic medical records EMR, which is available currently, or which may be created, used in the future. This policy applies to all faculty, staff, students, residents, and non-employees (Business Associates) who collect, maintain, use, or transmit EMR in connection with activities for UCR Health.

II. Definitions

Refer to Standard Definition Guide Document.

III. Policy Text

A. It is the legal and ethical responsibility of all UCR Health personnel, Medical School staff, faculty, residents, volunteers, students and researchers to protect the privacy and confidentiality of patients' protected electronic health information (ePHI). Only those individuals with a need to access and use an individual patient's protected health information in order to perform their required duties are permitted to do so.

B. Accessing the electronic medical record without proper authorization or outside of one's job responsibilities is considered a violation of this policy and will result in corrective action which may include termination of employment and personal legal consequences. Protected health information is to be maintained with appropriate security to prevent unauthorized access.

IV. Procedures

A. Individuals/Entities Allowed Access to the electronic Medical Record

1. Authorization to access EMR will be obtained through the Helpdesk ticket requesting system and the Compliance department and will be granted based on employment responsibilities. Level of access will also be granted based on job duties.
2. Supervisor/department head must send a request, opening a ticket in the Helpdesk system, complete the Authorization for EMR Access Form and return it to Compliance office.
3. Treating physicians, clinical staff and administrative staff will be given the level of assess needed to carry out their portion of a patient encounter.

4. UCR Health staff will be granted "staff" access as needed to execute daily healthcare operations (such as billing, coding, charge capture, risk management, quality and safety oversight, compliance, case management and utilization review).
5. Faculty, residents, students in the School of Medicine, nursing staff, other ancillary medical staff, and others designated by the Institutional Review Board (IRB) will be eligible to utilize medical records after receiving approval through the Authorization for Limited EMR Access form from the Compliance Office. Use of Protected Health Information for research must also have the written approval of the IRB.
6. Use for teaching purposes requires a UC teaching affiliation agreement or other legal agreement that describes the teaching relationship. The minimum necessary standard applies in this case. This access would also require an approved Authorization for Limited ERM Access form

B. Access Limitations

1. All access to EMR must only occur in UCR SOM and UCR Health locations during scheduled work hours.
2. Access is permitted for scope of work only. Access is never allowed for personal purposes such as reviewing records for self, family, friends, etc.
3. Upon change of duties or termination of employment the access to EMR will be terminated and no attempts should be made to further access the EMR system.
4. Patient Care Purposes
   a. Clinical Staff will have access only to the amount of information needed to treat the patient (Physician, PA/NP, Nurse, Staff) and attempts to access system elements beyond that scope of service should not be attempted.
   b. Staff will be permitted access to patient information only to the extent needed to complete their job responsibilities.
5. Non-Patient Care Purposes
   Staff access is limited to the amount of information necessary to perform necessary non-patient care required functions (payment and or operational purposes).
6. Research
   a. Access only to the amount of information needed to satisfy the project and as authorized by the IRB and approved through the Authorization for Limited EMR Access.
   b. At no time will patient identifiable information be released in any format in the results of the reported/published research project.
7. Vendor/BA access to UCR Health EMR will be authorized in the scope of the agreement and limited to the duties therein.

C. Possible Consequences of Unauthorized Disclosures

1. Unauthorized, willful disclosure of PHI or willful disclosure of PHI for personal gain could subject the individual to disciplinary actions up to and including termination and potential legal liability.
2. The HIPAA Privacy Rule 45 C.F.R. 164.530 and the Confidentiality of

Medical Information Act (Civil Code Section 56 et. Seq.) govern the release of patient identifiable information by hospitals and other providers. The Lanterman Petris Short Act protects the information of patients admitted to the psychiatric unit and psychiatric outpatient practices. These laws establish protections to preserve the confidentiality of medical information and specify that healthcare providers may not disclose medical information or records unless the disclosures are authorized by law or by the patient. This includes any information which identifies a patient by any one of the 18 HIPAA defined identifiers.

3. The medical record is a confidential and privileged document and can only be released in accordance with the Confidentiality of Medical Information Act (CMIA) and the HIPAA Privacy Rule. It is therefore the responsibility of UCR Health to safeguard the information in the medical record against loss, defacement, tampering or use by unauthorized persons.
    a. Records are to be treated as confidential material and protected for the sake of the patient and the institution.
    b. No one is permitted access or use beyond the extent that their job requires.
    c. PHI is not to be discussed among co-workers or shared with individuals or other third parties who are not permitted or authorized under law to receive the information.
    d. Confidentiality of information also applies to information that is retained in or printed from any computerized system.

D. Access to Electronic Medical Record (EMR)

1. System access requested for non-patient care purposes will be reviewed by Compliance and Privacy Officer and requests must be submitted 7 days in advance. (Attachment A: Authorization for Employee EMR Access Form)
2. System access will be granted in accordance with Access to Electronic Medical Record Policy and Procedure.

V. Forms/Attachments:

Attachment A – Authorization for Employee EMR Access Form
Attachment B – Policy Implementation Guidelines

VI. Related Information:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates significant changes in the legal and regulatory environment governing the provision of health benefits, the delivery of payment for healthcare services, and the security and confidentiality of individually identifiable, protected health information (PHI) in written, electronic or oral formats. The HIPAA Privacy Rule provides for the privacy of an individual's health information. The HIPAA Security Rule provides for the security of an individual's health information when the information is transmitted electronically. Title 22 requires that a written organizational policy exists that requires that medical records may be removed from the organization's jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute.

California Medical Information Act California Civil Code §56 outlines the California Requirements for protection of medical information in the state.

VII. Revision History: 3/2016

Approval(s):

Compliance Committee (04/26/2016)

Attachment A

Authorization for EMR Access

Please select whether you will require Full or Limited Access

☐ **Full Access**

Employee's Name: _____ Title: _____
☐ New Hire ☐ Position Change

Start Date: _____ End Date: _____

Level of Access Required: ☐ Physician ☐ Nurse ☐ Staff ☐ Admin

☐ **Limited Access**

Requestor's Name: _____

Date Access Needed: _____ Termination Date: _____

Reason for Request to Access EMR: _____
_____

Scope of Request (Include specific records, scope of review, amount of time needed in the system): _____
_____
_____
_____

Supervisor's Approval
Signature: _____ Date: _____

Compliance Approval
Signature: _____ Date: _____

Attachment B

POLICY IMPLEMENTATION GUIDELINES
HIPAA: CONFIDENTIALITY OF
PROTECTED HEALTH INFORMATION
(PHI)

In an effort to facilitate the implementation of the revised policy regarding confidential information, the Compliance and Privacy Officer in conjunction with the Vice Chancellor and Dean of the School of Medicine hereby provided the following implementation guidelines. They are intended to comply with 45 C.F.R. sections 164.306 and 164/308 et seq.

Licensed and credentialed UCR Health practitioners and students or trainees under their direct supervision may view abstracts of material containing protected health information ("PHI") upon an affirmative showing of good cause, and then only for purposes of direct patient care (e.g. preparation of progress notes, operative notes, discharge summaries, etc.) If a personal electronic device is used for anything other than access to electronic medical records through UCR Health approved firewalls and security measures, such device must meet the requirements of paragraph (4) below.

If questions arise regarding who or what circumstances are covered, the Compliance and Privacy Officer, in consultation with the Chair of the department of the involved practitioner, will make the final determination regarding access to PHI materials.

POLICY IMPLEMENTATION GUIDELINES

A. PHI may be retained by authorized personnel in the context of an IRB-approved clinical research study according to, and abiding by, safeguards as outlined by the IRB and UC policies.

B. The policy regarding confidential information is intended to prohibit all practitioners, students and/or trainees from maintaining ANY PHI on personal devices or media including blackberries or similar devices, cell phones and/or personal computers, etc., unless such device is certified by the University of California, Riverside School of Medicine Office of Information Services as being password protected with any information related to PHI being stored on that device sufficiently encrypted as to prevent disclosure of the PHI in the event the device is lost, stolen or the information stored within in otherwise compromised.

C. The term "clinical practice site" as used in the policy regarding confidential information is intended to encompass and apply to any and all clinical or office sites operated by or under the auspices of The Regents of the University of California, related in any way to the provision of clinical health care to individuals. Such sites include, but are not limited to: hospital-based clinics and laboratories; physician-based clinics and laboratories; outpatient surgery centers that exist or may in the

future exist, physician offices, whether or not located in space owned by The Regents of The University of California; research laboratories that may be repositories for PHI in any way; student health center; and counseling centers.

D. It is important to emphasize that it is the intent of the new policy and implementation guidelines to hold individuals accountable if any PHI is accessed beyond the premises of UCR Health clinical practice sites in any form by any employee, student, or trainee, or by any Business Associate within the scope of their agreement, and such PHI is lost, stolen or otherwise misplaced without adhering to the clarification and implementation guidelines set forth above.