Responsible Officer:	Vice Chancellor and Dean
Responsible Office:	University of California, Riverside School of Medicine
Origination Date:	06/2013
Date of Revision:	N/A
Scope:	UCR Health shall apply appropriate sanctions against Workforce members who fail to comply with UC Riverside Health's privacy policies and procedures, security polices and procedures for protection of ePHI or who fail to comply with the University of California's Policies on Information Security.

I. Policy Summary

UCR Health shall apply appropriate sanctions against Workforce members who fail to comply with UC Riverside Health's privacy policies and procedures, security policies and procedures for protection of ePHI or who fail to comply with the University of California's Policies on Information Security.

In order to reduce the likelihood of breaches, and in the event of intentional misconduct, repeated violations, or after corrective actions have failed to address the problem, the University will initiate appropriate disciplinary actions in compliance with University of California policies.

II. Definitions

Protected Health Information (PHI): is any individually identifiable health information regarding a patient's medical or physical condition or treatment in any form created or collected as a consequence of the provision of health care, in any format including verbal communication.

Electronic Protected Health Information (e-PHI): is any electronic information that is created or received by a health care provider that relates to the past, present, or future physical or mental health of an individual, and identifies the individual. This includes ePHI that is created, received, maintained or transmitted. For example, ePHI may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

Workforce: means all employees, volunteers, affiliate staff and other persons whose conduct, in the performance of their work for UCR Health, is under the direct or indirect control of UCR Health or the Regents of the University of California. Workforce includes all employees, medical staff, and other health care professionals, agency, temporary, contract, and registry personnel, trainees, house staff, students and interns, regardless of whether they are UC Riverside trainees or rotating through UCR Health facilities from another institution.

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, including medical information

Breach: is defined as the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information. Unauthorized acquisition, access, use or disclosure of encrypted ePHI does not constitute a breach.

Unauthorized: means the inappropriate access, review, or *viewing* of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use as permitted by California Medical Information Act (CMIA) or any other statute or regulation governing the lawful access, use, or disclosure of medical information. (California Health and Safety Code Sec. 2 §1280.15)

Medical Information: is defined as any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. (California Civil Code §56.05)

Individually identifiable: means that the 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, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

III. Policy Text

A. ***Potential breaches of electronic health information, and potential violations of the Privacy or Security Rule or related University policies for maintaining appropriate protections of electronic protected health information and/or restricted information must be reported through any one of the following mechanisms:***
   - ***Directly to the Compliance and Privacy Officer (951)827-4672***
   - ***Directly to the Director of Learning Technologies (951)827-2483***
   - ***Or through the compliance office confidential hotline (800) 403 4744 .***

1. <u>The potential or suspected security and/or privacy breach will be investigated by the Compliance and Privacy Officer and/or Security Officer to verify whether a violation actually occurred, and the extent of the violation.</u>
   a) *Findings from the investigation will be referred to the Human Resources Department, Chair or Residency Director, Executive Dean, and/or Dean of Student, as applicable, for determination of appropriate corrective and disciplinary action.*
      1) If the breach is confirmed, the Compliance and Privacy Officer and Security Officer, in conjunction with the Vice Chancellor and Dean of the School of Medicine, the Executive Dean, Department Chair, the employee's supervisor, Human Resources, Risk Management, and/or Campus Legal Counsel (as applicable) will evaluate the severity of the violation as follows:
         a) A minor breach that is accidental, non-malicious in nature, and/or due to lack of privacy or security training. Examples may include but are not limited, distributing email messages to the wrong individual unintentionally, disposing of patient information in an unsecured trash receptacle, or failure to secure information in a reasonable manner that allows inadvertent access to patient information by others.
         b) A moderate breach in which there has been disregard of University policy, or in which the intent of the violation is unclear and the evidence cannot be clearly substantiated as to malicious intent. Examples may include but are not limited to: sharing computer passwords, failing to log off computer systems, using another co-worker's password, failing to encrypt ePHI on mobile devices, or a repeated minor violation.
         c) A severe breach in which the employee purposefully or maliciously violates a patient's privacy or disregards University policy. Examples include, but are not limited to, releasing or using data for personal gain, destroying or falsely altering data, purposefully attempting to gain access to restricted information to which the employee does not have a work related need to access, maliciously attacking or hacking university systems, releasing patient data with the intent to harm an individual or the University, or a repeated moderate violation.
         d) Disciplinary action, up to and including termination, will be taken for any workforce member for a violation of privacy and security policies and procedures. University policy prohibits the use of University property for illegal purposes and for purposes not in support of the mission of the

University. In addition to legal sanctions, violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to University policies and collective bargaining agreements. Further information on permitted and prohibited uses is given in University of California Office of the President Electronic Communications Policy Section III, Allowable Use.

e) In the event that there is a determination that a potential crime has been committed, UC Riverside Police Department will be notified in consultation with UCR Campus Legal Counsel.

f) The Compliance and Privacy Officer will coordinate notification of patients with the department involved in the privacy breach within 5 days of the validation of the breach, and will coordinate notification to the applicable external regulatory agencies. (Refer to the UCR Health Policy "Privacy and Security Breach Response & Breach Notification Plan" for notification plan).

g) If the violation includes a potential breach of electronic information that triggers a notification requirement to the effected individuals, the policy on breach notification UCR Campus Policy 400-6, *Notification of security Breaches Involving Personal Information*, will also be followed.

h) If the violation involves a Business Associate as identified under the Health Insurance Portability and Accountability act, and UCR Health is unable to terminate the business associate relationship, a pattern of privacy and or security breaches may also be reported to the Office of Civil Rights for the Department of Health and Human Services.

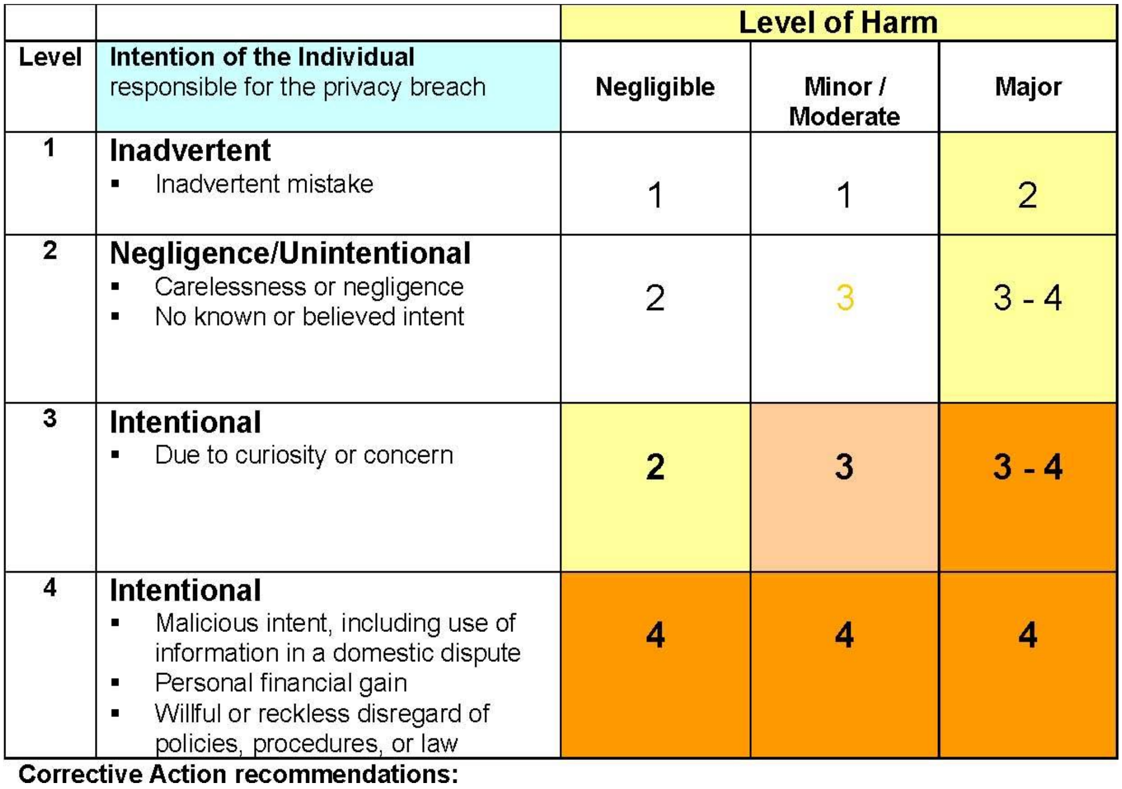
IV. Responsibilities: N/A

V. Procedures: N/A

VI. Forms/Instructions:

Privacy/Security Program: Incident Severity Scale

Guidelines will recommend corrective actions, once an incident and individual are identified. Nothing in these guidelines is intended to interfere with or limit employees' due process rights under law or policy. Any discipline recommended by these guidelines is subject to those due process rights.



		Level of Harm		
Level	**Intention of the Individual** responsible for the privacy breach	Negligible	Minor / Moderate	Major
1	**Inadvertent** ▪ Inadvertent mistake	1	1	2
2	**Negligence/Unintentional** ▪ Carelessness or negligence ▪ No known or believed intent	2	3	3 - 4
3	**Intentional** ▪ Due to curiosity or concern	**2**	**3**	**3 - 4**
4	**Intentional** ▪ Malicious intent, including use of information in a domestic dispute ▪ Personal financial gain ▪ Willful or reckless disregard of policies, procedures, or law	**4**	**4**	**4**

Corrective Action recommendations:

When determining the appropriate corrective action, additional factors that should be considered include previous history of corrective action (level of action may increase based on repeat offenses), and an inadvertent mistake based on a situation or operation that the individual did not know caused the breach.

Actions:

1. Re-training and/or counseling memo
2. Counseling memo, verbal warning, warning letter, or suspension (length to be determined by circumstance)
3. Suspension, or written warning indicating that any further conduct resulting in a breach of privacy will result in termination
4. Termination

Key to "Level of Harm":

Negligible: No effect on patient or organization; no apparent risk of harm.

Minor/Moderate: Minor or moderate harm (or potential harm) to patient, groups of patients and/or organization; may effect the community image of the organization.

Major: Major harm (or potential harm) to the patient, groups of patients and/or organization; may involve external media or government agencies. (Major harm examples: clear violation of privacy regulations; adverse publicity impact on patient; results in identity/medical identity theft).

VII. Contacts:

Unit	Title	Phone	
Compliance	Compliance Officer	(951) 827-4672	
Compliance	Privacy Analyst	(951) 827-7672	
Information Services	Director	(951) 827- 2483	

VIII. Related Information

Literature: Health Insurance Portability and Accountability Act, 45 CFR Sections 160-164 California SB 541 and AB 211 California Health and Safety Code Section 2 §1280.15 UC HIPAA Committee: Guidelines for Disciplinary Action for Privacy Violations.

California Civil Code – Sections 1798.29 and 1798.82

University of California: Electronic Communications Policy, November 17, 2000. Policies Applying to Campus Activities, Organizations, and Students, August 1994. Information Resources & Communications, Protection of Personal Information

UCR Health Privacy and Security Policies
Confidentiality of Confidential Patient Information
Safeguarding of Protected Health Information
Use of Patient Identifiable Information on Portable Computing and Electronic Storage Devices

UC Business and Finance Bulletins IS-3, Electronic Information Security IS-10, Systems Development and Maintenance Standards RMP-8, Legal Requirements on Privacy of and Access to Information

UCR Administrative Policies & Procedures Section 400-60, **Computing**.

IX. Revision History: N/A

Approval(s);

James R. Herron, Compliance and Privacy Officer
School of Medicine

G. Richard Olds, M.D.
Vice Chancellor and Dean, School of Medicine