Current Status: *Active*		**PolicyStat ID:** *3133792*
	Effective Date:	*4/20/2005*
	Review Date:	*12/30/2016*
	Revised Date:	*12/30/2016*
	Next Review:	*12/30/2016*
	Owner:	*Ann Chang: Dir*
	Policy Area:	*Compliance*
	Reference Tags:	
Ronald Reagan UCLA Medical Center	**Applicability:**	*Ronald Reagan UCLA Medical Center* *Ambulatory Care - UCLA* *Resnick Neuropsychiatric Hospital* *Santa Monica UCLA Medical & Orthopaedic* *UCLA Health*

Privacy and Information Security Sanction Policy, HS 9461

PURPOSE

The purpose of this policy is to describe the sanctions to be taken against Workforce members who fail to comply with UCLA Health Sciences privacy and information security policies and procedures.

SCOPE

This Policy applies to all faculty, staff, employees, students, trainees, and volunteers of the Ronald Reagan UCLA Medical Center, the Santa Monica UCLA Medical Center and Orthopaedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics and the David Geffen School of Medicine at UCLA (hereafter referred to as "UCLA Health Sciences").

DEFINITIONS

"Business Associate" means a person, contractor, supplier, institution or other entity that on behalf of the UCLA Health Sciences, but other than in the capacity of a Workforce member, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, consulting as further defined in HS Policy No. 9430, "*Business Associates*."

"Workforce" means employees, volunteers, and other persons whose conduct, in the performance of their work for UCLA Health Sciences, is under the direct control of UCLA Health Sciences or the Regents of the University of California, whether or not UCLA Health Sciences pays them. The Workforce includes employees, faculty, medical staff, and other health care professionals, agency, temporary and registry personnel, and trainees, housestaff, students and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health Sciences facilities from another institution.

POLICY

UCLA Health Sciences shall apply appropriate sanctions against Workforce members who fail to comply with UCLA Health Sciences Privacy and Information Security policies and procedures.

PROCEDURE

In order to reduce the likelihood of future errors, and in the event of intentional misconduct, repeated violations, or after corrective actions have failed to address the problem, the University may initiate disciplinary actions.

The Office of Compliance Services - Privacy and Information Security in conjunction with Human Resources will investigate all cases of alleged non-compliance with UCLA Health Sciences Privacy and Information Security policies. Cases for which sanctions may be appropriate will be brought forward to the Privacy and Information Security Disciplinary Action Committee for recommendations on disciplinary actions. Relevant laws, regulations and UCLA Health Sciences policies and procedures will be considered.

For individuals subject to its authority, the University shall impose disciplinary action in accordance with the rules set forth in the Faculty Code of Conduct, the Medical Staff Bylaws, Rules and Regulations, as well as any other existing and applicable personnel policies, collective bargaining agreements, University policies or guidance documents. Employees should review these and other personnel policies for a comprehensive description of disciplinary policies and procedures, including their rights under such circumstances.

Sanctions may include, but are not limited to:

- Counseling
- Suspension
- Fines
- Termination

For Business Associates and other third parties, the Office of Compliance Services - Privacy and Information Security will work with the appropriate UCLA department to implement any compliance corrective action or sanctions recommendations. These actions may include, but are not limited to, the removal of an individual third party employee or contractor from the UCLA contract or the termination of the UCLA third party agreement.

Any sanctions that are applied will be documented by the appropriate governing body for the workforce member or by the Office of Compliance Services - Privacy for contractors and Business Associates.

QUESTIONS

Workforce members should consult the Office of Compliance Services – Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu) if they have any questions on this policy.

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
University of California HIPAA Administrative Requirements
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Electronic Communications Policy (ECP)

CONTACT

Chief Privacy Officer, Office of Compliance Services
Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Approved:	February 22, 2006
Effective Date:	April 20, 2005
Review Date:	July 25, 2012, November 16, 2016
Revised Date:	November 2005; June 21, 2007; May 30, 2008, March 31, 2011 August 31, 2012, December 30, 2016

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010, 06/27/2012

Johnese Spisso, RN, MPA
President and CEO
UCLA Health System

Christopher Tarnay, M.D.
Chief of Staff
Ronald Reagan UCLA Medical Center

Roger M. Lee, M.D.
Chief of Staff
Santa Monica-UCLA Medical Center and Orthopaedic Hospital

Robert Suddath, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA

Attachments:

No Attachments