Current Status: *Active*		**PolicyStat ID:** *3133997*
	Effective Date:	*4/8/2003*
	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*

Mitigation Policy, HS 9490

PURPOSE

To establish the policy and procedure for the mitigation of any harmful effects of a violation of Privacy or Information Security policies regarding the uses and disclosures of Restricted Information by a UCLA Health Sciences Workforce member or by a Business Associate or other third party.

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").

POLICY

UCLA Health Sciences will mitigate, to the extent possible, any harmful effects of a violation of our Privacy and Information Security policies and procedures, or a California or federal law concerning the use or disclosure of Restricted Information by a member of our Workforce or by a Business Associate or other third party.

DEFINITIONS

"Protected health information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper, or oral. "Individually identifiable" means that the health or 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, genetic or other information that, alone or in combination with other

publicly available information, reveals the individual's identity. PHI includes: medical information; patient billing and health insurance information; and applies to a patient's past, current or future physical or mental health, or treatment.

"Electronic Protected Health Information" or "ePHI" is PHI that is transmitted by electronic media or is maintained in electronic media. For example, ePHI includes all data that may be transmitted over the Internet, or stored on a computer, a CD, a disk, magnetic tape or other media.

"*Personal Information (PI)*" as used in this policy means either of the following:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted:
    A. social security number,
    B. driver's license number or California identification card number,
    C. account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account,
    D. medical information,
    E. health insurance information; or
    F. information or data collected through the use or operation of an automated license plate recognition system as defined in California Civil Code §1798.90.5; or
2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

"***Medical Information***" means any individually identifiable information, in either electronic or physical form, regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and which may be in the possession of or derived from a health care provider, health care service plan, pharmaceutical company or contractor.

"*Health insurance information*" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

"Restricted Information" (as defined by UC Policy IS-3, Electronic Information Security) 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. This includes Personal Information, PHI and ePHI as defined in this section but could also include other types of information such as research data.

"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.

PROCEDURE

I. **Reporting Suspected Violations**
Any report or concern relating to a potential or suspected violation of privacy rights, either by a Workforce member or a Business Associate or other third party, should be promptly referred to the Chief Privacy Officer (*see*: HS Policy No. 9459, "*Privacy and Information Security Incident Reporting*").

II. **Investigation, Evaluation and Mitigation**

A. The Chief Privacy Officer or designee will investigate and gain a full understanding of the potential problem to determine whether the report or concern can be substantiated. If the report or concern is substantiated to have occurred, the Chief Privacy Officer will consult with the Chief Compliance Officer, Chief Compliance Security Officer, and/or Chief Information Security Officer to determine the extent of the harmful effect of the violation.

B. An evaluation by the Chief Privacy Officer, the Chief Compliance Security Officer, and Risk Management, in consultation with Legal Affairs, will be conducted to determine the following factors in whether or how to mitigate any damages:

i. Whether any damage occurred;

ii. The type and amount of damage, if any;

iii. The Restricted Information that was used or disclosed;

iv. The reason for the use or disclosure;

v. How the harm can be mitigated including, but not limited to notification of the individual(s).

C. The Chief Privacy Officer and Chief Information Security Officer will direct any necessary mitigation actions. The Chief Privacy Officer and Chief Information Security Officer, and/or their designee(s) will also:

i. Determine, how, when and why the problem arose;

ii. Review current policies and procedures;

iii. Determine how to correct the problem and prevent a recurrence;

iv. Determine what, if any, corrective, remedial or educational action is appropriate;

v. Determine if other corrective or disciplinary action is warranted in accordance with HS Policy No. 9600, *"Responding to Compliance Issues"* and HS Policy No. 9461, *"Privacy and Information Sanction."*

III. **Business Associates and other third parties**

A. If the harmful effects of the use or disclosure of protected health information were determined to be caused by a Business Associate or other third party, the Chief Privacy Officer or designee, will contact the Business Associate or third party to develop a mitigation plan.

B. UCLA Health Sciences does not have a responsibility to directly monitor the activities of its Business Associates or third parties. However, if a pattern of repeated violations by a particular Business Associate or third party is discovered, corrective actions will be determined by the Chief Privacy Officer. Corrective action may include termination of the contract. UCLA Health Sciences will notify the Office for Civil Rights of the Department of Health and Human Services of the violations if the contract for a Business Associate cannot be terminated.

IV. **Consultation**

The Chief Privacy Officer, or designee, should consult with Risk Management and/or the Health Sciences Office of Legal Affairs if he/she has any questions about potential liability or legal questions related to implementing the procedures described in Sections II and III above.

V. **Enforcement**

Failure to follow any provisions of this policy may result in disciplinary action, up to and including termination.

VI. **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.

REVISION HISTORY

Approved:	April 8, 2003
Effective Date:	April 14, 2003
Review Date:	November 16, 2016
Revised Date:	May 7, 2007, May 2 2008, March 31, 2011, December 30, 2016

CONTACT

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

REFERENCES

Health Insurance Portability and Accountability Act, 45 CFR 160-164
California Medical Information Act, California Civil Code Section 56 *et seq.*
Information Practices Act of 1977, California Civil Code, §§1798.29 and 1798.82
California Health and Safety Code, §§1280.15 and 130203

APPROVAL

Health Sciences Enterprise Compliance Oversight Board
Approved 12/11/2010

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