Current Status: *Active*		**PolicyStat ID:** *3136229*
	Effective Date:	*4/14/2003*
	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*

Privacy and Information Security Workforce Training, HS 9460

PURPOSE

The federal Health Insurance Portability and Accountability Act (referred to as "HIPAA" or the "Privacy Rule") requires that a covered entity must train all members of its Workforce on its policies and procedures with respect to Protected Health Information (PHI). This training must be conducted at a level appropriate for the members of the Workforce to carry out their job duties within the covered entity.

In addition, the HIPAA Security Rule requires that a covered entity must implement a security awareness training program on safeguards all Workforce members must use in protecting PHI in an electronic format (ePHI).

University of California Business and Finance Bulletin IS-3, *"Electronic Information Security"*, also requires security awareness training for all members of the University Community that should include practices established for safeguarding Restricted Information.

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

"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.

"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, or consulting as further defined in HS Policy No. 9430, "*Business Associates*."

"Observers" are individuals visiting UCLA Health Sciences (not family and friends visiting patients) who will be in contact with patients or exposed to patient information, including but not limited to observers of medical procedures and film crews.

"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

I. All UCLA Health Sciences Workforce members will be trained on the Privacy and Information Security Policies and Procedures (the "Policies") at a level appropriate for their job responsibilities. The training must be documented.

II. All new hires will be provided training during the hiring and orientation process.

III. Department-specific training on the Policies will be provided and documented as necessary by the applicable supervisor and/or department manager.

IV. Completion of the UCLA Health Sciences Confidentiality Agreement is required for all Workforce members at the time of orientation. Confidentiality Agreements will be completed and maintained in each Workforce member's personnel file.

V. Non-Workforce members such as Business Associates and Observers who are physically on UCLA Health Sciences premises and may be in contact with patients or patient information may also be required to take UCLA Health Sciences Privacy and Information Security Training. All such non-Workforce members and Observers will be required to sign the UCLA Health Sciences Confidentiality Agreement.

VI. In addition, Workforce Members will complete all training required by UCLA and UCOP as specified.

PROCEDURE

I. **Initial Training and Confidentiality Agreement**

A. Newly Hired Employees (except for Medical Staff)

i. Newly hired employees will complete the online Privacy and Information Security training module no later than five (5) business days after the hire date. Completion will be tracked by Human Resources (HR). Although Departmental Authorizers may approve and submit requests for computer accounts for access to Restricted Information prior to the completion of the online training, UCLA Health Sciences IT groups are not permitted to

issue a user logon and password information to such computer systems without confirmation that training has been completed.

ii. Newly hired employees will be provided with additional Privacy and Information Security training through the New Employee hiring process and/or the orientation sessions at the first available session after hire but in no case more than 45 days after hire and/or transfer into a covered position. Newly hired employees will sign the Confidentiality Agreement within 45 days of hire. The forms will be maintained in the employee's Personnel folder.

B. New Volunteers

i. New volunteers must complete the online Privacy and Information Security training module before they begin volunteering. Volunteers will give their certificate of completion to the Volunteers Office as evidence that the training has been completed. The certificate of completion will be placed in their volunteer file. Completion of the online training will be tracked by Human Resources.

ii. New Volunteers will sign the Confidentiality Agreement which will be maintained in their volunteer file.

C. Medical Students

i. New medical students must complete the online Privacy and Information Security training module as part of the annual School of Medicine orientation session. Completion of the online training will be tracked by Human Resources.

ii. Medical Students will sign the Confidentiality Agreement and it will be maintained with their student records.

D. Residents and Fellows

i. When residents and fellows first start at UCLA Health Sciences they must complete the online Privacy and Information Security training module before they are issued computer accounts that allow them access to Restricted Information. Completion of the online training will be tracked by Human Resources.

ii. Residents will sign the Confidentiality Agreement and it will be maintained with their personnel record.

E. New Medical Staff

i. New medical staff will be referred by Medical Staff Services to complete the online Privacy and Information Security training module during the initial Medical Staff credentialing process. If individuals do not complete the training prior to being appointed to the medical staff, their privileges will be immediately suspended until the training is completed. Note, UCLA Health Sciences does not allow transfer of HIPAA training credit from other institutions.

ii. Once the new medical staff complete the online training, they must forward the signed Confidentiality Agreement to Medical Staff Services.

F. Observers

i. Observers who will be at UCLA Health System for more than one week shall complete the online Privacy and Information Security training module on their first day. Completion of the online training will be tracked by Human Resources.

ii. All observers, regardless of the length of time they will be observing at UCLA, must also sign the UCLA Health Sciences Confidentiality Agreement. The signed forms will be maintained by the business unit where the observation will occur.

G. Temporary staff

i. Temporary staff will sign the UCLA Health Sciences Confidentiality Agreement and be provided training on the Policies by the agency or registry with which UCLA Health Sciences contracts for temporary services. The temporary service agencies and registries will be provided with copies of the UCLA Health Sciences training materials.

ii. The supervisor or manager of the department or area utilizing the temporary staff will confirm that the temporary staff have completed their training prior to starting their job duties and being authorized access to systems with Restricted Information.

H. Business Associates

i. Contractors or suppliers who will need to use or disclose PHI must sign HIPAA Business Associate Agreements (*see*: HS Policy No. 9430 "*Business Associate Agreements")*. Business Associates are required to provide HIPAA Privacy and Security training to their employees.

ii. For any UCLA Health Sciences-specific Privacy and Information Security requirements applicable to their contracted responsibilities, the Director of the Department contracting for their services will be responsible for providing and documenting the additional training.

iii. Business Associate staff who come onsite and will have access to PHI will be asked to sign the UCLA Health Sciences Confidentiality Agreement to remind them of their responsibility to protect patient privacy. The signed forms will be maintained by the business unit where the onsite work will be done.

II. **Ongoing Training**

A. Supplemental Privacy and Information Security Training

i. Supplemental training topics may include additional information on privacy requirements and patient's rights, roles of Workforce members, details on specific disclosure requirements and reporting privacy concerns.

ii. In addition to the online Privacy and Information Security training, managers, leaders, and Department Chairs or designee(s) are responsible for any additional Privacy and Information Security training that may be appropriate for targeted groups of Workforce members based on role-based job functions.

Possible topics for supplemental training include:

a. Provider issues

b. PHI Management for Data Stewards

c. Research

d. Fund-raising and Institutional Advancement

B. The Office of Compliance Services - Privacy and Information Security will provide ongoing Privacy and Information Security awareness training which may include:

i. Custom training sessions upon request (contact PrivacyInfoSec@mednet.ucla.edu)

ii. Awareness bulletins

iii. Online training materials and other Privacy and Information Security information

iv. Presentations

C. Supervisors and Managers will ensure that staff in their areas are kept up to date on department-specific Privacy and Information Security Issues.

D. Attendance at training sessions should be documented to allow UCLA Health Sciences to accurately reflect all Privacy and Information Security training a Workforce member has received. Providers of training should check with Human Resources on possible options for documenting training centrally to facilitate storage and retrieval of training records.

III. Privacy and Information Security Educational Resources

A. Answers to many Frequently Asked Questions (FAQ) can be found online on the Office of Compliance Services - Privacy and Information Security web site. http://compliance.uclahealth.org/body.cfm?id=189

B. General information on Privacy and Information Security is available online at the Office of Compliance Services - Privacy and Information Security web site: http://compliance.uclahealth.org/body.cfm?id=65

C. Follow the instructions below to find links to all the Privacy and Information Security policies on the UCLA Health Sciences Policy Site:

i. Start at the Mednet home page, http://www.mednet.uclahealth.org

ii. Under **System Resources**, click on **UCLA Health Systems Policies**

iii. Click on **Westwood - UCLA policies POLICYSTAT**

iv. In the **Policy Area** tab, double click on **Compliance** click on Search Policies.

v. After a couple of seconds, the bottom of the page with show links to all the Office of Compliance Services policies.

IV. Oversight Responsibilities

A. **Chief Privacy and Chief Compliance Security Officers**. The Chief Privacy and Chief Compliance Security Officers (or designees) will oversee the development of Privacy and Information Security education content and training materials, monitor compliance with training requirements through Human Resources, managers and supervisors. The Chief Compliance Officer or the Chief Privacy and Chief Compliance Security Officers will include a summary of compliance with the Privacy and Information Security training program

requirements in UCLA Health Sciences annual report of compliance activities. The status of training and will be reported on a periodic basis to the Compliance Committees.

B. **Managers and Supervisors**. Directors, managers, supervisors and Department Chairs (or their Designee) are responsible to:

   i. Monitor Workforce members in their area of responsibility to ensure all staff completes applicable Privacy and Information Security training modules, either online or in paper format. Monthly reports will be provided by Human Resources for training completed online.

   ii. Document and retain any additional training records related to compliance with Privacy and Information Security, including attendance at department meetings and completion of advanced module training as applicable, for a minimum of 6 years. Departments should check with Human Resources on possible options for documenting training centrally to facilitate storage and retrieval of training records. Copies of the actual training material should be maintained by the Department for 6 years.

V. **Sanctions for Failing to Take Training**

A. Completion of Privacy and Information Security training will be included on the monthly HR Competency tracking reports distributed to Department Managers and Directors as a mandatory completion item.

B. Individuals other than Salaried Academic and Staff Physicians: If it is discovered that a user has been granted access to a system without completing the required online training, the user's access privileges will be suspended until the training is completed unless the suspension would result in patient care/safety issues.

C. Members of the Medical and Professional Staff: Failure by any member to complete training will result in suspension of admitting and procedural privileges. Privileges will be reinstated upon completion of the Privacy and Information Security training.

D. Salaried Academic and Staff Physicians: Failure by any physician/provider to complete training may result in suspension of admission privileges and/or suspension of professional fee billing privileges. Admitting privileges and/or professional fee billing privileges will be reinstated upon completion of the Privacy and Information Security training.

VI. **Document Retention**

All documentation related to the completion of Privacy and Information Security training by the UCLA Health Sciences will be maintained for a minimum of 6 years. The responsible departments identified in this policy shall maintain a record of the online training records or records from training provided during the new employee orientation process.

VII. **Enforcement**

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

VIII. **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.

IX. **Policy Exceptions**

Unless an exception process is specified elsewhere in this policy, any exceptions to this policy must be for a valid patient care or business reason and must be approved by the Chief Compliance Officer or his/her designee. The Chief Compliance Officer or designee will consult with the appropriate business, leadership and IT groups in evaluating any proposed exceptions. The exception request form can be found at http://compliance.uclahealth.org/workfiles/PDF2/HIPAA%20Privacy/HIPAA%20Forms/General%20Exception%20Request%20form.pdf

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 Sections 1798.29 and 1798.82
California Health and Safety Code Section 1280.15
University of California HIPAA Administrative Requirements
University of California Business and Finance Bulletin IS-3, Electronic Information Security
University of California Los Angeles, Policy No. 401, Minimum Security Standards for Network Devices
University of California Los Angeles, Policy No. 404, Protection of Electronically Stored Information

CONTACT

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

REVISION HISTORY

Approved:	April 8, 2003; February 22, 2006
Effective Date:	April 14, 2003
Review Date:	July 25, 2012, November 16, 2016
Revised Date:	April 1, 2005; November 2005; May 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