Current Status: *Active*		**PolicyStat ID:** *5019599*
	Effective Date:	*4/20/2005*
	Review Date:	*7/2/2018*
	Revised Date:	*7/2/2018*
	Next Review:	*7/1/2021*
	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 Monitoring and Auditing Policy, HS 9462

PURPOSE

The purpose of this policy is to describe the requirements for monitoring and auditing UCLA Health Sciences Electronic Information Resources for potential threats and vulnerabilities to the confidentiality, integrity and availability of 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").

In addition, it applies to suppliers, contractors and other non-workforce members who are allowed access to UCLA Health Sciences Electronic Information Resources or Restricted Information and to any devices, including personally owned devices that store Restricted Information.

POLICY & PROCEDURE

I. As appropriate, UCLA Health Sciences Electronic Information Resources and personally owned devices connecting to UCLA Health Sciences Electronic Information Resources will be monitored for external and internal attempts at system disruption, unauthorized access, unauthorized use of Restricted Information, compliant configuration, contamination with malicious software and other intrusion efforts.

II. Electronic applications containing Restricted Information should log user access to Restricted Information. If an application includes auditing functions to log access to Restricted Information, the auditing functions must be enabled.

III. Access auditing is a required feature for new software and/or systems containing e-PHI and must be included in contracts and agreements. Applications maintained by Business Associates will also be required to maintain access logs and to provide access reports when requested by UCLA Health Sciences.

IV. UCLA Health Sciences shall maintain logs to track access and system configuration changes (syslogs, event logs and other system logs) for systems with e-PHI.

V. UCLA Health Sciences should maintain logs to track access and system configuration changes (syslogs, event logs and other system logs) for systems with Restricted Information and also for critical infrastructure.

VI. UCLA Health Sciences shall maintain audit logs of access to e-PHI, such as those generated by applications involving patient information, for a minimum of 6 years.

VII. Where feasible, proactive monitors will be implemented to flag access to the e-PHI of Persons of Interest for Office of Compliance Services - Privacy review to ensure appropriateness of access. Routine audits to detect unauthorized access to e-PHI as well as audits in response to specific patient complaints or concerns will be conducted under the direction of the Chief Privacy Officer.

VIII. For reporting integrity and availability, audit logs are to be maintained centrally. When this is not feasible, System Administrators are responsible to make sure procedures are in place to ensure the integrity and availability of the audit records.

IX. For existing legacy systems that do not have audit logs, remediation measures must be implemented and can include measures such as minimizing the number of authorized users to the system, restricting the application to a secure subnet, limiting physical access to the system or application or other reasonable technical and/or physical measures.

X. Security or Privacy incidents detected through auditing and monitoring activities must be reported to UCLA Health IT Customer Care at (310) 267-CARE (x7-2273), the Office of Compliance Services - Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu), and their supervisor(s). (*See* HS Policy No. 9459, "*Privacy and Information Security Incident Reporting*" and HS Policy No. 9461, "*Privacy and Information Security Sanctions").*

XI. Random and/or periodic audits may be conducted as necessary by Authorized Personnel to ensure the security, privacy, integrity and availability of all UCLA Health Sciences data and information systems and ensure compliance with UCLA Health Sciences policies.

XII. For more information on auditing and monitoring activities and the investigations or actions that may result from auditing and monitoring, see HS Policy No. 9451, "*Use of Electronic Information by the UCLA Health Workforce (Employees)*."

XIII. Any additional technical requirements of the Health Sciences Privacy and Information Security Auditing and Monitoring Standard must also be followed.

XIV. Enforcement

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

XV. 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. Exceptions may be requested by submitting an exception request form.

XVI. 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
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 Sections 1280.15, 123148 and 130203
California Lanterman-Petris Short Act ("LPS Act")
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; June 21, 2007,
Review Date:	July 25, 2012
Revised Date:	May 30, 2008, March 31, 2011, August 31, 2012, June 29, 2018

APPROVAL

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

Johnese Spisso, RN, MPA
President UCLA Health
CEO UCLA Hospital 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

Laurie R. Casaus, M.D.
Chief of Staff
Resnick Neuropsychiatric Hospital at UCLA

Appendix I – Definitions

"Electronic Information Resources" includes, but is not limited to, computer equipment (servers, workstations, laptops and other portable computers), online services, medical devices, mobile devices (tablets ,smart phones, digital cameras, etc.), applications (Electronic Health Record, email, databases, other software), storage media (USB drives, DVDs, CDs, magnetic tape, memory cards), and networks.

"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:

A. 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:
    1. social security number,
    2. driver's license number or California identification card number,
    3. 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,
    4. medical information, or
    5. health insurance information, or
    6. information or data collected through the use or operation of an automated license plate recognition system as defined in the California Civil Code §1798.90.5; or
B. 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.

"Authorized Personnel" means the UCLA IT Health, or Office of Compliance Services personnel designated to follow up on issues involving use of Electronic Information Resources.

"Persons of Interest" are patients who may require ongoing monitoring of access to their PHI because they are high profile individuals, persons of interest to the media, UCLA employees in highly visible roles and other UCLA employees or any patients that have special concerns about their privacy or have been victims of a previous privacy incident or identity theft.

"Security Incident" is the attempted or successful unauthorized access to, use, disclosure, modification, or

destruction of information or interference with system operations in an information system. (45 C.F.R. section 164.304).

"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.

Attachments:

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval	Johnese Spisso: Ceo Med Ctr [MW]	7/2/2018
Administration Approval	Christopher Tarnay: Hs Assoc Clin Prof-Hcomp [MW]	7/2/2018
Administration Approval	Roger Lee: Hs Clin Prof-Hcomp [MW]	7/2/2018
Administration Approval	Laurie Casaus: Hs Assoc Clin Prof-Hcomp [MW]	7/2/2018
Executive Medical Boards - MSEC, RNPH PSEC, SMEMB	M. Lynn Willis: Mgr	7/2/2018
Hospital System Policy Committee Chair	M. Lynn Willis: Mgr	6/21/2018
Hospital System Policy Committee	M. Lynn Willis: Mgr	6/21/2018
	Ann Chang: Dir	6/2/2018

Applicability

Ambulatory Care - UCLA, Resnick Neuropsychiatric Hospital, Ronald Reagan UCLA Medical Center, Santa Monica UCLA Medical & Orthopaedic, UCLA Health