Current Status: *Active* **PolicyStat ID:** *8252094*

Effective Date:	*04/2005*
Approved Date:	*07/2020*
Revised Date:	*07/2020*
Next Review:	*07/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Information Security Policy, HS 9450

PURPOSE

This policy sets forth guidelines for securing and maintaining the confidentiality, integrity and availability of electronic information as required by University policies and the Administrative Simplification requirements contained in the federal Health Insurance Portability and Accountability Act (referred to as the "Security Rule").

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.

DEFINITIONS

"Protected Health Information" or "PHI" is any individually identifiable health information, in any form or media, whether electronic, paper or oral, regarding a patient created as a consequence of the provision of health care. "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.

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.

"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, house staff, students, and interns, regardless of whether they are UCLA trainees or rotating through UCLA Health Sciences facilities from another institution.

POLICY/PROCEDURE

All members of the UCLA Health Sciences Workforce are responsible for securing and maintaining the confidentiality, integrity and availability of Restricted Information. The UCLA Health Sciences policies, the University of California policies, and the UCLA policies listed below apply to all Workforce members and non-workforce members who are allowed access to UCLA Health Sciences Electronic Information Resources or Restricted Information.

I. **University of California-wide Policies**

A. **Business and Finance Bulletin IS-3, Electronic Information Security:** This is the University of California best practice Information Security policy which applies to the entire University of California System.

B. **Electronic Communications Policy (ECP):** This policy clarifies the principles of academic freedom, shared governance, freedom of speech, and privacy as they relate to electronic communications. The ECP establishes a high standard for the nonconsensual access to an individual's electronic communications and requires that each campus establish implementation guidelines to ensure compliance with its provisions.

II. **UCLA Information Security Policies**

A. **UCLA Policy 401, *"Minimum Security Standards for Network Devices"***: All devices connecting to a Campus Network must comply with the best practice Minimum Security Standards defined in this policy, which includes keeping operating system patches up to date, using anti-malware software and keeping it current, running host-based firewalls, and disabling all unnecessary services.

B. **UCLA Policy 404, *"Protection of Electronically Stored Information"***: Personal Information in the custody or control of UCLA should only be electronically stored when there is a reasonable academic or business purpose, and if so stored, it must be encrypted or otherwise protected against loss or theft of the data and/or System.

III. **UCLA Health Sciences Privacy and Security Policies**
These policies were originally developed to address the Administrative, Physical and Technical safeguards to protect PHI and ePHI as required by the HIPAA Security Rules and have been extended as appropriate to apply to Restricted Information. Brief descriptions of the policies that are most relevant to Information Security are listed below.

A. **Protection and Use of PHI**
Members of the UCLA Health Sciences Workforce may not disclose, share, or otherwise use any individually identifiable Medical Information except for Treatment, Payment and Health Care Operations (referred to hereafter as "TPO") unless expressly authorized by the patient or otherwise permitted or required by law (*see*: HS Policy No. 9401, *"Protection and Use of PHI" and* HS Policy No. 9421*, "Access to and Use of PHI")*.

B. **Use of University Electronic Information Resources by UCLA Health Sciences Workforce Members**
UCLA Health Sciences Electronic Information Resources are the property of UCLA Health Sciences and may only be used for the work-related business activities and operations of UCLA Health Sciences. All UCLA Health Sciences Workforce members must comply with the guidelines for the acceptable utilization of Electronic Information Resources as set forth in HS Policy No. 9451, "*Use of Electronic Information Resources by UCLA Workforce (Employees*)" and in other University Policies.

C. **Minimum Security Standards**
All devices connecting to UCLA Health Sciences networks or storing UCLA Health Sciences Restricted Information must be configured according to minimum security standards (*see:* HS Policy No. 9457, *"Minimum Security Standards"* and UCLA Policy No. 401, *"Minimum Security Standards")*. Devices include, but are not limited to: computers, servers, laptops, tablets, smart phones, web servers, databases, file and other application servers, and medical and other devices, both physical and virtual, both on and off premises.

D. **Users Accounts and Identity Management**
All members of the UCLA Health Sciences Workforce should only have access to Restricted Information as necessary for their job functions. UCLA Health Sciences shall determine which individuals are authorized to work with Restricted Information, including but not limited to ePHI, in order to carry out their job responsibilities. UCLA Health Sciences shall establish unique user identification for each individual who is authorized to access Restricted Information, including but not

limited to ePHI. (See: HS Policy No. 9421, "*Workforce (Including Employee) Access to and Use of PHI (Minimum Necessary Standard)*" and HS Policy No. 9452, "*User Accounts (Authorizing Access to Restricted Information; Passwords."*)

E. **Requests to Download or Interface**

Requests by UCLA Health Sciences Workforce members or Departments to conduct data downloads and/or interfaces with other systems/users that involve Restricted Data must be approved in advance by the UCLA Health Sciences Office of Compliance Services Privacy and Information Security Officers or their designees as set forth in HS Policy No. 9454, "*Requests to Interface or Download Restricted Information.*"

F. **Security Assessment**

UCLA Health Sciences shall conduct risk assessments to identify the electronic information resources that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability of Restricted Information. Risk assessments should include a gap analysis to identify necessary remediation opportunities. (*See*: HS Policy No. 9455, "*Security Assessment and Management.*")

G. **Physical Security**

UCLA Health Sciences shall select appropriate mechanisms to physically safeguard Restricted Information in any form, including, but not limited to computing devices, electronic storage media, paper, and any other devices that store, transmit, or access Restricted Information (*see*: HS Policy No. 9456, *"Physical Security of Restricted Information")*.

H. **Fax**

The transmission of Restricted Information via facsimile (fax) is permissible in situations in which the information is required for continuity of patient care, for payment of patient accounts or other healthcare and business operations. Only the information minimally necessary to accomplish the purpose should be transmitted. (*See*: HS Policy No. 9453-B, *"Facsimile Transmission of Restricted Information."*)

I. **Mobile Devices**

All Mobile Devices and Removable Media used for University Business must be encrypted and password protected. (*See*: HS Policy No. 9453-C, *"Storage and Use of Restricted Information on Mobile Devices and Removable Media"* and UCLA Policy No. 404*, "Protection of Electronically Stored Information.")*

J. **Backup and Contingency Plans**

UCLA Health Sciences shall conduct back up of data and software on an established schedule. Backup copies should be stored in a physically separate location from the data source. UCLA Health Sciences shall ensure that business continuity planning includes measures to recover from a disaster that renders resources unavailable within an acceptable period of time. Disaster recovery plans must be tested on a periodic basis or in response to major changes to the working environment. UCLA Health Sciences will also establish contingency plans ("down-time procedures") to ensure ongoing access to ePHI and mission critical Restricted Information for patient care and business purposes during periods of temporary loss or unavailability of computer infrastructure. (*See*: HS Policy No. 9458, "*Backup and Contingency Plans.*")

K. **Electronic Mail (Email)**

UCLA Health Sciences shall educate staff about the risks of email. Sending Restricted Information via email should be limited, particularly when transmitting email outside of the UCLA Health Sciences Mednet network. UCLA Health Sciences shall alert patients to the risks of unsecured email. As reasonably practical, UCLA Health Sciences shall consider alternative secure email/web messaging solutions for direct patient communication. All archived email files containing Restricted Information should be secured. (*See:* HS Policy No. 9453-A, *"Use of E-Mail in Communication of Restricted Information.*")

L. **Remote Access**
All remote access across the Internet into UCLA Health Sciences networks should be approved in advance by authorized personnel and accomplished using UCLA-issued VPN software or other approved methods. (*See:* HS Policy No. 9453-D, *"Remote Access.*") The security configuration of the remote device must comply with all UCLA Health Sciences security policies, including HS Policy No. 9451, "*Use of Electronic Information*;" HS Policy No. 9457, "*Minimum Security Standards;*" UCLA Policy No. 401, *"Minimum Security Standards;"* and UCLA Policy No. 404, *"Protection of Electronically Stored Information."*

M. **Privacy and Information Security Incident Reporting**
All UCLA Health Sciences Workforce members shall report security incidents as described in HS Policy No. 9459, "*Privacy and Information Security Incident Reporting.*"

N. **Workforce (Employee) Training and Education**
All UCLA Health Sciences Workforce members will be trained on the Privacy and Information Security Policies and Procedures at a level appropriate for their job responsibilities. The training must be documented. (*See*: HS Policy No. 9460, "*Privacy and Information Security Workforce Training.*")

O. **Privacy and Information Security Sanction Policy**
UCLA Health Sciences shall take disciplinary action against Workforce members who fail to comply with University policies and procedures, including information security policy and procedures, in accordance with University personnel policies and collective bargaining agreements. (*See*: HS Policy No. 9461, *"Privacy and Information Security Sanctions.*")

P. **Monitoring and Auditing**
UCLA Health Sciences will implement hardware, software and/or procedure mechanisms that record and examine activity in information systems that contain or use Restricted Information. Audit logs of confirmed security incidents shall be maintained for six (6) years. (*See*: HS Policy No. 9462, "*Privacy and Security Monitoring and Auditing.*")

Q. **Agreements with Third Parties**
UCLA Health Sciences must enter into University-approved Business Associate Agreements (or amendments) with its business associates and obtain documented satisfactory assurance that the business associate will appropriately safeguard any ePHI or PHI provided under the business associate arrangement. (*See*: HS Policy No. 9430, *"Business Associates*.")

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

V. **Questions**
An employee who is uncertain about a particular Information Security requirement or UCLA Health Sciences Information Security policy should consult with his/her supervisor. The supervisor should refer any questions regarding the security question to their local IT or Technical support, or to the UCLA Health Sciences Office of Compliance Services - Privacy and Information Security (**CompOffice@mednet.ucla.edu**).

VI. **Exceptions to Policy**

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.

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

University of California Business and Finance Bulletin IS-3, Electronic Information Security

University of California Electronic Communications Policy (ECP)

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

University of California Los Angeles, Policy No. 420, Notification of Breaches of Computerized Personal Information

CONTACT

Chief Privacy Officer, Office of Compliance Services

Chief Compliance Security Officer, Office of Compliance Services

Revisions: 12/2016, 12/2019

All revision dates:	07/2020, 12/2016, 03/2011, 05/2008, 06/2007, 11/2005

Attachments

No Attachments

Approval Signatures

Step Description	Approver	Date
Administration Approval- President and CEO, UCLA Health	Johnese Spisso: Ceo Med Ctr [JB]	07/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	07/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	07/2020

Step Description	Approver	Date
Resnick Neuropsychiatric Medical Staff Executive Committee- Chief of Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	07/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	07/2020
Policy Owner	Liangzhou Chen: Mgr	06/2020