Effective Date:	*04/2005*
Approved Date:	*09/2020*
Revised Date:	*09/2020*
Next Review:	*09/2023*
Owner:	*Liangzhou Chen: Mgr*
Policy Area:	*Compliance*
Reference Tags:	*Lippincott*
Applicability:	*Ronald Reagan, Resnick, Santa Monica, Ambulatory Care*

Security Assessment and Management, HS 9455

PURPOSE

This policy sets forth guidelines for conducting security assessments in order to evaluate, remediate and manage potential risks to the confidentiality, integrity and availability of Restricted Information ("Security Assessment") as required by the Administrative Simplification requirements contained in the federal Health Insurance Portability and Accountability Act (referred to as the "Security Rule") and the University of California Business and Finance Bulletin IS-3, Electronic Information Security.

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 Orthopedic Hospital, the Resnick Neuropsychiatric Hospital at UCLA, the Faculty Practice Group, all ambulatory clinics, the David Geffen School of Medicine, UCLA School of Nursing, UCLA School of Dentistry, and UCLA Fielding School of Public Health (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 format, including verbal communications. "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, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. PHI includes 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 is an individual's first name or first initial and last name combined with any one of the following:

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.

"***Medical Information***" means any 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. Medical information and health insurance information for patients are also considered to be PHI.

"Restricted Information" 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.

"Risk" is the likelihood of a given threat triggering or exploiting a particular vulnerability and the resulting impact on the organization.

"Threat" is the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

"Vulnerability" is a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

POLICY

I. **Introduction**
UCLA Health Sciences shall conduct ongoing Risk Assessment to develop and maintain an Security Risk Management Plan to identify and reduce risks.

II. **Security Assessment**

A. UCLA Health Sciences will perform ongoing Risk Assessments to accurately and thoroughly assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of the Electronic Information Resources held by the organization.

B. Risk Assessments may be performed at different levels of the organization, including:

i. Enterprise-wide

ii. For individual departments or units

iii. For new systems, applications, and interfaces, or existing ones with any significant changes in

functionality or types of data used. (Detailed requirements for this level of Risk Assessment are in HS Policy 9457 "*Minimum Security Standards: Health Sciences Risk Assessment Standard*")

C. An Enterprise-wide Risk Assessment should be conducted at a minimum annually either internally or by an independent contractor, using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and/or focusing on the Health Insurance Portability and Accountability (HIPAA) Security and Health Information Technology for Economic and Clinical Health (HITECH) Act requirement.

   i. The Office of Compliance Services - Information Security, working with UCLA Health IT Security, will finalize the documentation for the Risk Assessment and report the results to Management. The results provide the basis for the Security Management Plan.

III. **Security Management Plan**

UCLA Health Sciences must implement administrative, physical, and/or technical measures that reduce the risks to its information systems containing e-PHI and Restricted Information to reasonable and appropriate levels.

A. The data from the Risk Assessments will be used to conduct a gap analysis of security measures, policies, and procedures.

B. The Office of Compliance Services - Information Security, working with UCLA Health IT Security resources and other stakeholders, will identify remediation opportunities, which may include identification and implementation of policies and procedures, administrative solutions (including training), and technical solutions.

C. UCLA Health IT Security and the Office of Compliance Services - Information Security, working with UCLA Health IT Security resources, shall track and document remediation, and provide reports on status to Management.

D. Office of Compliance Services - Information Security reserves the right to audit networks and systems on a periodic basis to ensure policy compliance.

IV. **Questions**

For questions, contact the Office of Compliance Services - Information Security (CompOffice@mednet.ucla.edu).

V. **Enforcement**

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

VI. **Policy Exceptions**

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

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

University of California Electronic Communications Policy (ECP)

University of California HIPAA Information Security Policy

National Institute of Standards and Technology Special Publication (SP) 800-3

CONTACT

Chief Privacy Officer, Office of Compliance Services

Chief Information Security Officer, Office of Compliance Services

REVISION HISTORY (PRE-POLICYSTAT)

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

All revision dates: 09/2020, 08/2012, 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]	09/2020
Ronald Reagan Medical Staff Executive Committee- Chief of Staff	Carlos Lerner: Assoc Prof Of Clin-Hcomp [JB]	09/2020
Santa Monica Medical Staff Executive Committee- Chief of Staff	Roger Lee: Hs Clin Prof-Hcomp [JB]	09/2020
Resnick Neuropsychiatric Medical Staff Executive Committee- Chief of Staff	Aaron Kaufman: Hs Assoc Clin Prof-Hcomp [JB]	09/2020
Hospital System Policy Committee Chair	Jeffrey Bergen: Mgr [KK]	07/2020
Policy Owner	Liangzhou Chen: Mgr	07/2020