LAC+USC MEDICAL CENTER POLICY

Subject:	Original Issue Date:	Policy #
SECURITY COMPLIANCE EVALUATION	7/13/10	**468**
	Supersedes: 9/22/17	Effective Date: 10/30/20

Departments Consulted:	Reviewed & Approved by:	Approved by:
Information Systems Office of Risk Management	Attending Staff Association Executive Committee Senior Executive Council	(Signature on File) Chief Medical Officer (Signature on File) Chief Executive Officer

PURPOSE

To establish a process for monitoring LAC+USC Medical Center compliance with the security aspects of the LAC+USC Policy No. 361.1, LAC+USC Privacy and Security Compliance Program.

POLICY

LAC+USC Medical Center must evaluate security safeguards to determine whether safeguards are in compliance with the requirements of the LAC+USC Medical Center Privacy and Security Compliance Program Policy. This evaluation must first occur at the completion of the implementation of LAC+USC's security safeguards.

On an annual basis, LAC+USC Medical Center must evaluate one or more of it is Information Systems. The sequence of evaluations must be prioritized as defined in the Application and Criticality Analysis in the LAC+USC Medical Center Policy No. 467, Facility Information Technology (IT) Contingency Plan. Each system selected for evaluation must have its security safeguards evaluated in each of the following categories:

A. Administrative
B. Physical
C. Technical

The purpose of this periodic evaluation is to demonstrate and document compliance with the LAC+USC Medical Center Privacy and Security Compliance Program Policies. These evaluations are necessary to determine the effectiveness of existing security safeguards in light of technological, environmental or operational changes. Any findings of noncompliance or security failures must be remedied in accordance with the Facility Master Security Management Report LAC+USC Medical Center Policy No. 461, Security Management Process: Risk Management.

DEFINITIONS

For a more complete definition of terms used in this policy and/or procedure, the DHS Information Security Glossary, Attachment I, (460-A) to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

PROCEDURE

The Departmental Information Security Officer (DISO) and Departmental Information Security Steering Committee (DISSC) are responsible for evaluating the security safeguards of each

LAC+USC' Information Systems to ensure compliance with LAC+USC Policy No. 361.1, LAC+USC Privacy and Security Compliance Program Policy.

I. Periodic Evaluation by the DISO

A. The Medical Center DISO or designee must prepare a written evaluation of the LAC+USC Facility's security safeguards including a review of the viability of LAC+USC Medical Center Privacy and Security Compliance Program Policy.

B. The Medical Center DISO's approval is required before any change developed and recommended by the DISSC is made to any security policy or security procedure.

II. Periodic Evaluation by the DISSC

A. The DISSC must review the DISO's report of the evaluation of the effectiveness of the technical and non-technical security safeguards and make all recommendations necessary for additions, modifications or deletions in the security policies and procedures.

B. If the DISSC preliminarily recommends a new security standard or a change in LAC+USC' Privacy and Security Compliance Program Policy, such new standard or change will be communicated by the DISO to the LAC+USC CIOs who will elicit feedback within a specific period of time and provide such feedback to the DISSC.

C. The DISSC will consider the feedback received and make a final recommendation on any suggested changes to the DISO.

D. Changes approved by the DISO must be communicated to the Facilities through policy updates and reminders. LAC+USC is required to update their security policies and procedures in a timely manner to incorporate all such changes.

E. Workforce members may suggest changes to the security policies or procedures by submitting suggestions to the Medical Center CIO, Assistant Departmental Information Officer (ADISO), the DHS DISO and/or the DISSC.

III. Evaluation Upon Occurrence of Certain Events

A. If one or more of the following events occur, the policy evaluation process described in Section II must be immediately implemented:

1. Changes in any of the regulatory, compliance and/or accreditation security regulations or privacy regulations.

2. New federal, state, or local laws or regulations affecting the privacy or security of confidential and/or sensitive information.

3. Changes in technology, environmental processes or business processes that may affect the LAC+USC' Privacy and Security Compliance Program Policy.

4. A serious security violation, breach, or other security incident occurs and the analysis conducted under LAC+USC Policy No. 935.06, Security Incident Report and Response indicates that policies and/or procedures need to be added or modified.

5. Changes in any County or LAC+USC policies and/or procedures that may affect the LAC+USC Privacy and Security Compliance Program Policy.

B. The DISO may reconvene the DISSC at the DISO's discretion.

IV. Evaluation of LAC+USC Procedures

Periodically, LAC+USC CIO/designee, must evaluate the security aspects of the LAC+USC Privacy and Security Compliance Program Policy, as applicable to the Facility; the Facility's own security policies and procedures, and the implementation, operation and maintenance of such policies and procedures. The purpose of such internal evaluation is to determine the Facility's compliance status and make any changes necessary in order to become compliant, and/or to demonstrate and document compliance with the LAC+USC Privacy and Security Compliance Program Policy and the Facility's own security policies and procedures.

V. Internal Audit of Security Policies and Procedures

All security-based policies and procedures, including the implementation, operation and maintenance of such policies and procedures, are subject to periodic audits by LAC+USC' Internal Audit department and/or DISO or designee.

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, § 164.308(a)(8), Administrative Safeguards; Standard: Evaluation
Board of Supervisors Policy No. 6.108, "Auditing and Compliance"

CROSS REFERENCES

DHS Policies: DHS Policy No. 361.1, DHS Privacy and Security Compliance Program Policy
DHS Policy No. 361.23, Safeguards for Protected Health Information
DHS Policy No. 935.00, DHS Information Technology and Security Policy
DHS Policy No. 935.07, Facility Information Technology (IT) Contingency Plan

REVISION DATES

February 11, 2014; September 22, 2017; October 30, 2020