LAC+USC MEDICAL CENTER POLICY

		Page 1	Of 3
Subject: **INFORMATION ACCESS MANAGEMENT**	Original Issue Date: 7/13/10	Policy # **464**	
	Supersedes: 9/22/17	Effective Date: 10/30/20	

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

PURPOSE

To create administrative controls for access to Protected Health Information (PHI) and other confidential and/or sensitive information. To restrict access to those persons and external entities with a need for access is a basic tenet of security.

POLICY

LAC+USC must ensure that Information Technology Management or designees establish procedures for access authorization, access establishment and access modification that restricts access to only those persons with a need for access to accomplish the essential tasks of their respective job functions LAC+USC must verify that a Business Associate Agreement with external entities to manage access authorization, access establishment and access modification is in place.

1. Access Authorization

LAC+USC must ensure that Information Technology Management authorize access to information resources under their control on a “need to know basis” for carrying out the essential job functions of the workforce members. Workforce members are prohibited from attempting to gain unauthorized access to confidential information. Information Technology Management must implement access control mechanisms for electronic systems to protect against unauthorized and inadvertent use, disclosure, modification, or destruction of resources.

Information Technology Management must set up authorization, establishment and modification procedures for controlling access to information. The DISO must assist Information Technology Management in implementing the access authorization procedures and determining the appropriate technical access controls.

2. Isolating Health Care Clearinghouse Function

After exercising due diligence, LAC+USC Medical Center has determined that it has no health care Clearing house as defined by HIPAA that is a part of its larger organization.

3. Access Establishment and Modification

Facility CIOs must ensure that Information Technology Management document and implement procedures for establishing LAC+USC workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.

Facility CIOs must ensure that Information Technology Management document and implement procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align each workforce member's access with the workforce member's essential job functions.

DEFINITIONS

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

PROCEDURE

1. Information Access Management

Facility CIO/designee must work with System Managers/Owners, LAC+USC managers and supervisors and LAC+USC Human Resources to develop information access procedures and to coordinate those activities necessary to implement the information access procedures.

The Information Technology Management must ensure that appropriate physical safeguards and technical security policies are established and enforced. The Information Technology Management must also ensure compliance with these polices is verified in such a manner and frequency that the purpose of this policy is demonstrably accomplished.

2. Elements

The information access management policy of each LAC+USC facility must include the following elements:

A. Access authorization
B. Access establishment and modification
C. Supervision of workforce members and others who do not have authorized access but work in locations where electronic data might be accessed.

3. Access Authorization

A. Each LAC+USC Medical facility must implement a facility-based procedure specifying how a person is granted authorization to access confidential information.

LAC+USC Medical Center must also specify in writing who may authorize such access, for what purposes access can be authorized, and the procedures for approving and documenting the access authorization. The specification must include how and when to modify or cancel such access and procedures for communicating such changes to appropriate people and systems. These specifications must also establish limits on access to confidential information based on the role(s) of the person (for example, a treatment provider generally needs access only to health information for people they are treating; a billing person needs only sufficient information to bill for work done, not full patient records, etc.). Access authorization must specify what authorized people may do with confidential information such as use (read), create, modify, and remove (delete).

B. The authorization criteria must include required levels of training and training certification requirements commensurate with the level of access. The access level must be established by a single point of approval, the System Manager/Owner or designee, and may be for a limited period of time. Renewal or a change of access level must require re-evaluation of access needs and may require continued or additional training.

4. Access Establishment and Modification

Each System Manager/Owner must specify in writing how to establish the access authorized. This must include specifying who is responsible for establishing the access, the procedures to be followed and how the granting of access must be documented.

Each System Manager/Owner must specify how to modify an access authorization including how to cancel an authorization. This includes who is responsible for establishing the change in authorization, the process for changing the authorization, and the process for documenting the changing of access.

AUTHORITY

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(2)
Board of Supervisors Policy Nos.: 6.100, “Information Technology and Security Policy”
6.101, “Use of County Information Technology Resources”

REFERENCES

DHS Policies 935.01 INFORMATION ACCESS MANAGEMENT

REVISION DATES

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