LAC+USC MEDICAL CENTER POLICY

Subject: **WORKFORCE SECURITY**	Original Issue Date: 7/13/10	Policy # **463**
	Supersedes: 9/22/17	Effective Date: 10/30/20

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

PURPOSE

To ensure LAC+USC workforce members have appropriate access to data systems and information contained in data systems and to prevent unauthorized access to confidential and Protected Health Information (PHI).

POLICY

It is the policy of the LAC+USC to ensure the security (confidentiality, integrity and availability) of PHI and other confidential information. LAC+USC will develop and implement security procedures that protect the confidentiality of PHI and other confidential information. Access will be granted based upon the workforce member's job responsibility and "need to know".

LAC+USC CIOs/designees must work with LAC+USC Information Technology Management and Human Resources to develop and coordinate implementation of the workforce security procedures.

LAC+USC Workforce Authorization and Supervision Procedure

LAC+USC Information Technology Management or designees must ensure that workforce members are granted access authorization in accordance with LAC+USC IS Policy 464, Information Access Management

The authorization and supervision process must consist of the following components:

1. LAC+USC Information Technology Management must identify and supervise workforce members who work with or have access to PHI and other confidential information. LAC+USC Information Technology Management must identify the minimum information access required by these workforce members to do their job.

2. LAC+USC Information Technology Managements or designees must identify the security levels necessary for securing the system and allow workforce members to perform their jobs. LAC+USC Information Technology Management will assign workforce members to the minimum security level that they need to perform their job function.

3. LAC+USC managers/supervisors must restrict access to PHI and other confidential information by unauthorized workforce members.

4. LAC+USC Information Technology Management must provide authorization and supervision to workforce members and others who need to be in areas where PHI and other confidential information may be accessed and take appropriate safeguards to ensure those who may be exposed to PHI and other confidential information are made aware of the policies protecting that information.

LAC+USC Workforce Clearance Procedure

LAC+USC Information Technology Management must ensure that workforce members' access to PHI and other confidential information is limited to the minimum necessary to perform their job responsibilities.

The clearance process must consist of the following components:

1. LAC+USC Information Technology Management or designee must work with Human Resources (HR) to ensure proper workforce clearance procedures are implemented. Refer to DHS Policy No. 703.1, Criminal Records Background Check/Fingerprinting Policy.

2. LAC+USC Information Technology Manage mentor designees must ensure all applications for access to a system are complete and approved by the appropriate workforce managers/supervisors. They must also ensure that each workforce member with access has signed the County Acceptable Use Policy agreement and an acknowledgment of LAC+USC Policy No. 457, Acceptable Use Policy for County Information Technology Resources that defines their responsibility for the protection of the confidentiality, integrity and availability of all LAC+USC information resources and restrictions for utilizing those resources. LAC+USC Human Resources must ensure that each new workforce member receives and signs the County Acceptable Use Policy agreement and an acknowledgment of LAC+USC Policy No. 457 during the new hire orientation and that each workforce member completes the agreement and the acknowledgment during the annual Performance Evaluation process. The signed agreement and acknowledgment will be filed in the workforce member's official personnel folder.

LAC+USC Workforce Termination Procedure (Access)

LAC+USC Information Technology Management must ensure that departing workforce members' access to all PHI and other confidential information is terminated upon termination of employment.

The termination process must consist of the following components:

HR terminates LAC+USC workforce members' access to all PHI and other confidential information upon termination of employment.

1. LAC+USC Information Technology Management must be notified by the workforce member's Supervisor when a workforce member's status/function/responsibility has changed. LAC+USC Information Technology Management must promptly review the workforce member's access to PHI and other confidential information and must modify the member's access as needed.

2. HR must terminate the workforce member's access to PHI or other confidential information upon notification by the workforce members or workforce member's supervisor when the workforce member terminates employment or transfers to another or County department. Access termination must be:

    a. As soon as possible but in no circumstance later than 5 business days when the end of employment is voluntary.

    b. As soon as possible but in no circumstance later than close of the same business day or end of workforce member's work shift when the end of employment is involuntary,

DEFINITIONS

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

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3)(ii)
Board of Supervisors Policy Nos.:6.100, "Information Technology and Security Policy"
6.101, "Use of County Information Technology Resources"

CROSSREFERENCES

DHS Policies:

361.8, "Minimum Necessary Requirements for Use and Disclosure of Protected Health Information (PHI)"
703.1, "Criminal Records Background Check/Fingerprinting Policy"
935.20, "Acceptable Use Policy for County Information Technology Resources"

REVISION DATES

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