LAC+USC MEDICAL CENTER POLICY

		Page 1	Of 3
Subject: **INFORMATION INTEGRITY**	Original Issue Date: 7/14/09	Policy # **476**	
	Supersedes: 9/22/17	Effective Date: 10/30/20	

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

PURPOSE

To protect Protected Health Information (PHI) and other confidential information from improper alteration and/or destruction.

POLICY

The LAC+USC must ensure that appropriate authentication mechanisms are utilized to corroborate that stored data within its possession has not been altered or destroyed in an unauthorized manner.

LAC+USC Information Technology Management are responsible for implementing integrity checks using the above referenced authentication mechanisms and reporting any suspicious findings to the LAC+USC CIO/designee. All workforce members must also report any unauthorized data modification or destruction to the LAC+USC Information Technology Management.

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.

PROCEDURES

The LAC+USC CIO/designee shall determine the need for integrity controls following the result of risk assessment, LAC+USC Policy No. 461, Data Security Management Process: Risk Management. The LAC+USC CIO/designee must ensure that general integrity control procedures and integrity checking procedures are implemented to protect PHI and other confidential information from improper alteration and/or destruction.

1. General integrity control procedures:

   The LAC+USC CIO/designee must:

   a. Ensure that information systems include integrity controls of all hardware and software.

   b. Ensure all integrity controls are documented in the System Security Documentation defined in LAC+USC Policy No. 474, System Access Control:

Definitions, and are reviewed and approved by the Departmental Information Security Officer (DISO) or designee.

c. Ensure workforce members are trained to maintain data integrity.

d. Examine workflow procedures and system components for reliability and correctness to guard against unauthorized modification or destruction of data.

e. Protect information systems against environmental threats that would harm data, including air temperature and humidity, fire suppression systems, or weather-related events.

f. Provide a means for employees to report suspected unauthorized data modification or destruction in accordance with LAC+USC Policy No. 466, Security Incident Report and Response.

2. Integrity checking procedures:

LAC+USC System Managers/Owners must:

a. Use the integrity controls listed in the Recommended Safeguards Description section of the Risk Management Report specified in LAC+USC Policy No. 461, Security Management Process: Risk Management.

b. Determine the directories and files for which data integrity will be checked including those containing PHI and other confidential information.

c. Establish a schedule for checking stored files in which the frequency of inspection is commensurate with the criticality of each file type including both periodic inspections and event specific checks (e.g., upon receipt or transmission of information).

d. Determine the integrity resources and methods that will be used to perform integrity inspections (e.g., cryptographic check sum tools, lists of directories and files and the attributes of each, log files detailing actions taken by users and virus scanners).

e. Create baseline reference information based on the integrity control(s) selected (e.g., cryptographic check sums) for the applicable directories and files. The preferred method for recording and accessing the baseline reference data is through a read only medium (e.g., CD-ROM). These records must be stored securely, accessible only to appropriate personnel and protected against environmental threats.

f. Check actual directory and file contents and attributes against the baseline reference(s) selected (e.g., cryptographic check sum matching) to determine if there have been any unauthorized (actual or suspected) changes to the system.

g. Report any unauthorized (actual or suspected) changes to the system by following LAC+USC Policy No. 466, Security Incident Report and Response.

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3) (ii)

CROSS REFERENCES

DHS Policies:
935.00 LAC+USC Information Technology and Security Policy
935.01 Data Security Management Process: Risk Management
935.06 Security Incident Report and Response
935.14 System Access Control

REVISION DATES

July 14, 2009; February 11, 2014; September 22, 2017; October 30, 2020