LAC+USC MEDICAL CENTER POLICY

Subject: **DATA SECURITY DOCUMENTATION**	Original Issue Date: 9/14/10	Policy # **479**
	Supersedes: 9/22/17	Effective Date: 10/30/20

Departments Consulted: Information Systems Health Information Management	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 establish documentation requirements for data security policies and procedures and for Health Insurance Portability and Accountability Act (HIPAA) Security Rule implementation decisions.

POLICY

1. LAC+USC DOCUMENTATION REQUIREMENT

   LAC+USC must develop and maintain data security policies and procedures in either paper or electronic form. All data security actions taken and assessments conducted by LAC+USC, as specified in the LAC+USC Policy No. 490, LAC+USC Privacy and Security Compliance Program, LAC+USC Policy No. 474, System Access Control and in any other related policies or procedures (security compliance documentation) must be documented and maintained in either paper or electronic form.

2. DOCUMENTATION RETENTION

   All data security documentation must be retained for at least 6 years (as required by the HIPAA Security Rule) from the date of its creation or the date when it last was in effect, whichever is later. If, however, LAC+USC is subject to a longer documentation retention period as a part of a regulatory, compliance and/or accreditation requirement [e.g., Medicare, Medi-Cal, JCAHO, Title 22] then the documentation must be retained for the longer period.

3. DOCUMENT AVAILABILITY

   The security policies and procedures must be made readily available to those Users who must comply, and to those persons who are responsible for ensuring or auditing compliance, with the security policies and procedures.

   Access to data security documentation must be strictly limited to those whose roles or titles have been identified by LAC+USC as having a business need to know and must be approved by the Departmental Information Security Officer (DISO). LAC+USC must ensure that the security compliance documentation is stored securely, and that only that security compliance documentation that is relevant and necessary is made available to those persons who have been authorized by the DISO.

4. UPDATES

Reports and data of Information security actions taken and assessments conducted must be archived in a security compliance documentation repository as soon as reasonably possible. Historical documentation of the security policies and procedures and the security compliance documentation repository must be preserved.

In accordance with the responsibilities assigned by LAC+USC Privacy and Security Compliance Program policies and procedures, the DISO and CIO or designees must review and revise the security policies and procedures in response to environmental or operational changes affecting the security of the computer information assets. See LAC+USC Policy No. 460, LAC+USC Information Technology and Security Policy and LAC+USC Policy No. 468, Compliance Evaluation.

DEFINITIONS

SECURITY COMPLIANCE DOCUMENTATION
Includes all documentation pertaining to security policies, procedures, actions taken, risk assessments and safeguards implemented in Information Technology systems (i.e., the System Security Documentation).

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.

AUTHORITY

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.316(b)(1)
Applicable Los Angeles County and DHS Policies and Procedures

CROSS REFERENCES

DHS Policies:
361.1, DHS Privacy and Security Compliance Program
935.00, DHS Information Technology and Security Policy
935.08, Security Compliance Evaluation
935.14, System Access Control

REVISION DATES

September 14, 2010; February 11, 2014; September 22, 2017; October 30, 2020