LAC+USC MEDICAL CENTER POLICY

Subject: **PERSON OR ENTITY AUTHENTICATION**	Original Issue Date: 9/14/10	Policy # **477**
	Supersedes: 9/22/17	Effective Date: 10/30/20
Departments Consulted: Information Systems Health Information Management Office of Risk Management	Reviewed & Approved by: Attending Staff Associations Executive Committee Senior Executive Council	Approved by: (Signature on File) Chief Medical Officer (Signature on File) Chief Executive Officer

PURPOSE

To verify that a person or entity seeking access to Protected Health Information (PHI) and other confidential information is the one claimed.

POLICY

LAC+USC CIO or designees must establish and document facility-based procedures for each of the following requirements and submit such procedures for approval to the Departmental Information Security Officer or designee.

1. A user authentication mechanism (e.g., unique user identification and password, biometric input, or a user identification smart card) must be used for all Workforce Members seeking access to any network, system, or application that contains PHI and other confidential information.

2. Two-factor authentication, in which the user provides two means of identification, one of which is typically physical (e.g., a secure ID card using a one-time code), and the other of which is typically something memorized (e.g., a secret Personal Identification Number (PIN)) is required for all systems receiving a Risk Analysis Sensitivity score of "HIGH," (LAC+USC Policy No. 461, Security Management Process: Risk Management), and for all remote access.

   Workforce Members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

   Users are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

   LAC+USC CIO or designees must ensure that users make a reasonable effort to verify the identity of the receiving person or entity prior to transmitting PHI and other confidential information.

   LAC+USC CIO or designees must ensure that the LAC+USC information technology managers implement the system authentication mechanism that is appropriate for the risk expected for the system. Information technology managers must document the selected system authentication mechanism in the System Security Documentation (LAC+USC Policy No. 474, System Access Control) that accompanies the electronic data system.

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.

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.312(d).
Board of Supervisor Policy Nos.:
6.100, Information Technology and Security Policy
6.101, Use of County Information Technology Resources

CROSS REFERENCES

DHS Policies:
361.24, Safeguards for Protected Health Information (PHI)
935.01, Security Management Process: Risk Management
935.03, Workforce Security
935.04, Information Access Management
935.14, System Access Control
935.20, Acceptable Use Policy for County Information Technology Resources

REVISION DATES

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