LAC+USC MEDICAL CENTER POLICY

		Page 1	Of 3
Subject: **DATA TRANSMISSION SECURITY**	Original Issue Date: 9/14/10 Supersedes: 9/22/17	Policy # **478** Effective Date: 10/30/20	
Departments Consulted: Information Systems 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 define the technical requirement that electronic information transmitted over a communications network must be protected in a manner commensurate with the associated risk.

POLICY

LAC+USC must maintain controls to ensure the integrity of information transmitted electronically within or outside of LAC+USC Information Resources, including public and private connections to any part of the LAC+USC communication network. Pursuant to the LAC+USC Risk Management Plan, LAC+USC Policy No. 461, Security Management Process: Risk Management, LAC+USC must deploy encryption whenever deemed appropriate to secure Protected Health Information (PHI) and other confidential communications transmissions.

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

The appropriate measure of transmission security necessary is determined through the Risk Assessment and Risk Management process as outlined in the LAC+USC Master Security Management Report, LAC+USC Policy No. 461, Security Management Process: Risk Management.

A detailed description of DHS network security methods for enforcing transmission security are stated in the DHS IT Network Security Architecture document and in the DHS IT Network Security Guidelines.

1. The Departmental Information Security Officer (DISO) or designee must ensure that LAC+USC deploys and maintains integrity controls and encryption to secure PHI and other confidential communications transmissions over the Internet, external connections and all parts of the communication network (i.e., Local and Wide Area Network, LAN, WAN and Wireless).

2. The DISO will provide oversight and guidance to the LAC+USC CIO or designees to deploy the appropriate network security methods stated in the LAC+USC Network Security Architecture and the LAC+USC IT Network Security Guidelines.

3. LAC+USC CIO or designees must ensure that the facility LAN is optimally managed, operational, secured and integrated into the LAC+USC WAN for secured Internet and external connections.

4. LAC+USC CIO or designees must ensure that the LAC+USC information technology managers utilize and maintain integrity controls and encryption whenever deemed appropriate to secure PHI and other confidential communications transmissions.

5. LAC+USC CIO or designees must ensure that the LAC+USC information technology managers take in consideration each system's Risk Analysis Sensitivity Score (LAC+USC Policy No. 461, Security Management Process: Risk Management) implement controls to ensure only authorized Workforce Members have access to network services for secured data transmission, LAC+USC Policy No. 474, System Access Control.

6. LAC+USC CIO or designees must ensure that the integrity controls and encryption implemented under this policy are documented within the System Security Documentation (LAC+USC Policy No. 474, System Access Control: Definitions).

7. LAC+USC CIO or designees must ensure that the LAC+USC information technology managers implement the following integrity control procedures.

   a. Identify the information communicated across networks, including all traffic containing PHI and other confidential information, for which data integrity will be checked.

   b. Determine the integrity controls (e.g., application or network message authentication tools) that will be used to perform the integrity inspections.

   c. Utilize the selected integrity controls to check the integrity of incoming PHI and other confidential messages.

   d. If the integrity controls identify a discrepancy between the message received and the message sent, or if it appears that no message authentication measure has been included, then the LAC+USC information technology managers must notify the appropriate LAC+USC CIO/designee.

8. LAC+USC CIO or designees must ensure that the LAC+USC information technology managers implement the following encryption procedures when deemed necessary pursuant to the LAC+USC Risk Management Plan;

   a. Determine the encryption mechanisms that will be used in transmitting or receiving PHI and other confidential information messages over an open communications network and ensure that such encryption mechanisms are compatible with the encryption features employed by entities with which the communicates.

b. PHI and other confidential messages requiring encryption must be encrypted at the application or network layer prior to being transmitted.

c. Ensure passwords, tokens and keys associated with the message encryption measures are protected from unauthorized disclosure or access in accordance with LAC+USC Policy No. 474, System Access Control: Encryption and Decryption Procedures.

AUTHORITY

45 Code of Federal Regulations, Part 164, Subpart C, Section 164.312(e)(1)

REFERENCES

DHS Policies:
935.01, Security Management Process: Risk Management
935.14, System Access Control
DHS Network Security Architecture
DHS IT Network Security Guidelines

REVISION DATES

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