LAC+USC MEDICAL CENTER POLICY

Subject:	Original Issue Date:	Policy #
SECURITY INCIDENT REPORT AND RESPONSE	7/13/10	**466**
	Supersedes: 8/16/17	Effective Date: 10/30/20

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

PURPOSE

To establish a policy to protect the integrity, availability and confidentiality of confidential or proprietary information, including electronic Protected Health Information (ePHI) and to outline LAC+USC's coordinated response to information system security incidents.

POLICY

It is LAC+USC policy to protect electronic confidential and patient information in compliance with state and federal laws, as well as industry best practices for identifying, tracking and responding to network and computer-based Information Technology (IT) security incidents.

LAC+USC Workforce Members are required to immediately report any actual or suspected security incidents, intrusion attempts, security breaches, theft or loss of hardware and any other security related incidents which violate the confidentiality, integrity, or availability of digital information to the Enterprise Help Desk (EHD).

Upon notification of an incident the EHD must create an EHD Ticket assigned to the Departmental Information Security Officer (DISO) and copied to the HSA Security Compliance Division at SecurityCompliance@dhs.lacounty.gov.

The Security and Compliance Division will investigate and, as needed, escalate, remediate, or refer to others. The DISO or designee and the Departmental Computer Emergency Response Team (DCERT) are responsible for determining the appropriate level of response to the security incident and completes an IT Security Incident Report. The LAC+USC Chief Information Officer (CIO) must ensure that the information technology managers respond in a manner authorized and directed by the DISO or designee and the DCERT.

The incident will be documented by providing a general description of events, approximate timelines, the parties involved, resolution of the incident, external notifications required and recommendations for prevention and remediation.

The DHS security incident reporting and response procedures to be followed, include the completion of the DHS Incident Report form. This is consistent with Board of Supervisor's Policy No. 6.103, Countywide Computer Security Threat Response.

DEFINITIONS

IT Security Incident ("Incident")
An incident is any activity that harms or represents a serious threat to the whole or part of the Department of Health Services (DHS) computer, and network-based resource(s) such that there is an absence of service, inhibition of functioning systems, including unauthorized changes to hardware, firmware, software or data, unauthorized exposure, change or deletion of PHI, or a crime or natural disaster that destroys access to or control of these resources. (refer to Incident Reporting Process Flow (Attachment I) and IT Security Incident Response Matrix (Attachment II)).

CCERT
The Los Angeles County Computer Emergency Response Team has responsibility for response and reporting of IT security incidents.

DCERT
The HSA Department Computer Emergency Response Team has responsibility for response and reporting of IT security incidents.

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

As required by the Policy section above, suspected and actual breaches of security must be reported to the Enterprise Help Desk. The Enterprise Help Desk will contact the DISO who will complete and submit a Security Incident Report (Attachment III to the HSA Security Compliance Division.

The process for responding to information security incidents includes:

- Identify and report the incident
- Validate the incident
- Evaluate the incident for the extent of its threat
- Take actions based on prioritization of assets and processes
- Re-evaluate and repeat actions until threat is controlled
- Inform workforce members and management, as necessary
- Document details, as appropriate
- Initiate long-term actions to reduce likelihood of recurrence, as appropriate

Workforce Members must report all potential information security incidents to the appropriate management personnel. A workforce member may not prohibit or otherwise attempt to hinder or prevent another Workforce Member from reporting an information security incident. Incidents may also be identified through automated processes such as periodic virus scans, intrusion detection analysis, firewall and other log analysis, and other appropriate audit mechanisms.

AUTHORITY

45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(6)(i)
Board of Supervisors Policy No. 6.103, "Countywide Computer Security Threat Response"

REFERENCES

DHS Policy 935.06 SECURITY INCIDENT REPORT AND RESPONSE

ATTACHMENTS

Attachment I: DSH IT Security Incident Reporting Process flow

Attachment II: Security Incident Response Matrix

Attachment III: IT Security Incident Report Form

REVISION DATES

February 11, 2014; August 16, 2017; October 30, 2020