LOS ANGELES GENERAL MEDICAL CENTER POLICY

	Page 1	Of 4
Subject: **SECURITY MANAGEMENT PROCESS: RISK MANAGEMENT**	Original Issue Date: 7/13/10	Policy # **461**
	Supersedes: 10/30/20	Effective Date: 4/9/24
Policy Owner(s): Chief Information Officer Executive Sponsor(s): Chief Executive Officer		
Departments Consulted: Information Systems Office of Human Resources	Reviewed & approved by: Attending Staff Association Executive Committee Senior Executive Officer	Approved by: (Signature on File) Executive Officer
		(Signature on File) Chief Executive Officer

PURPOSE

To create and implement information security management processes which ensure the security (confidentiality, integrity, and availability) of electronic Protected Health Information (ePHI) and other confidential data.

SCOPE

The Information Security Management process is intended to support Los Angeles General in actively managing and controlling information assets.

POLICY

Los Angeles General Medical Center must establish and maintain an Information Security Management Process. This process must be documented and auditable; and must include:

1. **Application/System Inventory**

   Inventory information should include hardware, software, system interfaces, data and information, people, and system mission. This information is needed to determine system boundary, functions, criticality, and sensitivity.

   Los Angeles General IT Operations must document application/system inventory in an approved Inventory Management Solution.

2. **Risk Analysis**

   Los Angeles General must ensure that System Managers/Owners conduct risk assessments that include physical, administrative, and technical controls to safeguard ePHI and other confidential data.

   System risks/vulnerabilities can be determined by using a host/network scanning tool approved by Los Angeles General.

Application risks/vulnerabilities can be determined by using an application vulnerability scanning tool approved by Los Angeles General.

System managers/owners must document their risk assessment.

3. Risk Management

Los Angeles General Medical Center must ensure that System Managers/Owners recommend safeguards and actions to mitigate those identified system and application vulnerabilities.

The Los Angeles General must ensure that System Managers/Owners develop appropriate plans to implement the recommended safeguards and actions.

4. Information Systems Activity Review

Los Angeles General Medical Center must ensure that System Managers/Owners establish, document, and implement procedures and schedules for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.

System Managers/Owners must document their system activity reviews

Los Angeles General must conduct an evaluation of their information security safeguards annually; or more frequently where there are changes in the Los Angeles General Facility's security environment to demonstrate and document their compliance with both the Los Angeles General' and the Board of Supervisors' security policies and procedures.

RISK

The potential for harm of loss. Risk is best expressed as the answers to these four questions:

1. What could happen? (What is the threat?)
2. How bad could it be? (What is the impact or consequence?)
3. How often might I happen? (What is the frequency?)
4. How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se?

RISK ASSESSMENT

The identification and study of the vulnerability of a system and the possible threats to its security.

SYSTEM CRITICALITY LEVEL

Mission Critical – Failure would preclude Los Angeles General entity from accomplishing its core business function(s)

Mission Important – Failure would not preclude Los Angeles General entity from accomplishing its core business functions in the short term (a few hours) but failure would preclude it from accomplishing its core business functions in the long term (a few hours to a few weeks)

Mission Supportive – Failure would not preclude Los Angeles General entity from accomplishing its core business function (s) in the short term or long term but would have an effect on day-to-day operations

DATA SENSITIVITY

High – The most sensitive unclassified data (other than unclassified data whose loss could adversely affect national security interests). This data requires the greatest number and most stringent information security safeguards at the user level.

Moderate – Data has importance to Los Angeles General and must be protected against such acts as malicious destruction. However, because this type of data is most often collected for analytical purposes, disclosure problems are not usually significant.

Low – Threats to this data are minimal and only minimal precautions to protect the data need to be taken. Unintentional alteration or destruction is the primary concern.

RISK MANAGEMENT

The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

THREAT

An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.

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 (CFR) Part 164, §164.308(1)(i)
Health Insurance Portability and Accountability Act of 1986 (HIPAA), 42 U.S.C. Sections 1320-d – 1320-d-8.
Board of Supervisors Policies:
6.100, “Information Technology and Security”
6.101, “Use of County Information Technology”
6.106, “Physical Security”

6.107, “Information Technology Risk Assessment

CROSS REFERENCES

DHS Policies
361.1, “DHS Privacy and Security Compliance Program”
361.10, “Disciplinary Actions for Failure to Comply with Privacy Policies and Procedures
747, “Disciplinary Action”
935.00, “DHS Information Technology and Security Policy”
935.06, “Security Incident Response and Reporting”

REVISION DATES

February 11, 2014; September 22, 2017; October 30, 2020; April 9, 2024