
TITLE: **INFORMATION SECURITY AUDIT AND EVALUATION**

POLICY:

Information systems maintain audit logs for information access and are periodically evaluated to measure effective security safeguards, including policies, controls and processes.

PURPOSE:

Evaluate security controls and processes associated with information systems in order to provide proper security.

APPLICABILITY:

Hospital staff, employees, owners, custodians, and users of information systems

PROCEDURE:

Audit Mechanisms

Regulations require audit of all access to sensitive data. Custodians and owners of information systems document and implement the audit mechanisms, frequency of log review, and log retention period determined as a result of the risk analysis.

1. The audit mechanisms implemented in information systems provide the following information for each auditable event:
   A. Date and time of activity
   B. Patient identifier
   C. Identification of user performing activity
   D. Description of attempted or completed activity
   E. Origin of activity (for example, IP address, workstation identifier, as available)

2. The audit mechanisms generate reports of auditable events. Examples include:
   A. Failed authentication attempts
   B. Unusual pattern of access to patient records
   C. Access to information systems

D. Information system start up or shutdown
E. Use of privileged accounts (for example, system administration account)
F. Security incidents
G. Changes to user's security information (for example, user privileges)
H. Vendor and temporary account activities
I. Use of audit software programs or utilities (for example, system logs)

3. Custodians follow *Audit Log Processing Procedure* to export application Audit Logs (and follow *Platform Audit Log Processing Procedure* for logs at the platform level). Log processing generates different reports that custodians review to monitor operational security status of their information assets. If necessary, they also conduct periodic self-audits.

   Audit log processing may generate alerts based on anomalies in access patterns, which are investigated and resolved by the Information Security Office and in communication with the Privacy Office as necessary.

4. Custodians review the audit mechanisms periodically. The risk analysis considers the following factors with respect to the frequency of reviews of audit mechanisms:
   A. The merit or sensitivity of the information system.
   B. The degree to which the information systems are connected to and dependent on other information systems and the degree to which the connection or dependency poses a security risk to the system.

Evaluation of Security Safeguards through Risk Analysis

5. Departments and workforce members are included in the Risk Analysis evaluation as appropriate, including:
   A. Information system or application owners and custodians
   B. Executive Management
   C. Legal Affairs
   D. Privacy Office, Corporate Compliance and Internal Audit Department

6. The evaluation may be conducted or certified by a third party if the Information Security Office deems it necessary and appropriate.

7. Each evaluation includes (see *Risk Analysis Procedure*):
   A. A review of security configuration and procedures to evaluate their appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of information systems.

B. An assessment and evaluation of security controls and processes as reasonable and appropriate protections against the risks identified for information systems.

8. Following each evaluation, security procedures, controls and processes are updated if the results of the evaluation show that such updates are required in order to protect against any reasonably anticipated threats or hazards.

Log-in Monitoring Process

9. The log-in process has the following attributes:
   A. Notification displays upon log-in stating that the system must only be accessed by an authorized workforce member.
   B. After maximum six (6) unsuccessful attempts to enter a password, the involved User Id must be either suspended until reset by a system administrator or service desk personnel, permitted temporary access with system custodian notification or temporarily disabled for no less than three (3) minutes.
   C. In order to minimize information exposure of extraneous information which could be used to attack a system, identification information (name, version, etc.) about information systems (hardware, operating system, databases, etc.) and applications should be avoided on sign on screens.
   D. The log-in process on information systems, has the ability to:
      a. Record failed log-in attempts.
      b. Upon completion of a successful log-in, record the date and time of the log-in.

Exceptions

10. To the extent the procedures in this policy are not followed, custodians document reasons for exception during the Risk Analysis.

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Audit Log Processing Procedure (IT-SEC-004)
Platform Audit Log Processing Procedure (IT-SEC-005)

Risk Analysis Procedure (IT-SEC-001)
Health Insurance Portability and Accountability Act of 1996, 45 CFR
164.308(a)(1)(ii)(D),
164.308(a)(5)(ii)(C),
164.308(a)(8),
164.312(b)

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: June 2013; **March 2015**