

UNC School of Medicine
Information Security Audit Policy

AUDIT TRAILS

- 1) **SUBJECT:** Audit trails must be maintained to provide accountability for the use of information resources within the UNC School of Medicine (UNC SOM).
- 2) **SCOPE:** This policy applies to all UNC SOM information systems containing Protected Health Information and Confidential Information as defined in the UNC Health Care System Information Security Statement and all information users.
- 3) **DESCRIPTION:** In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be maintained. This is used to investigate security incidents, monitor use of UNC SOM resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
- 4) **PROCEDURES & GUIDELINES:**
 - a) Audit Trails will be maintained for UNC SOM information systems:
 - (1) The following transactions must be logged for each server where technically and operationally feasible:
 - Server startup and shutdown
 - Account creation, modification, or deletion
 - Loading and unloading of services
 - Installation and removal of software
 - System alerts and error messages
 - User logon (failed and successful) and logoff
 - Accesses to sensitive information and systems
 - Modifications of privileges and access controls
 - (2) The following transactions must be logged for each application where technically and operationally feasible:
 - Modifications to the application
 - Account creation, modification, or deletion
 - Application alerts and error messages
 - User sign on (failed and successful) and sign off
 - Accesses to sensitive information
 - Modifications of privileges and access controls
 - (3) The following transactions must be logged for each router, firewall, or other major network device where technically and operationally feasible:
 - Device startup and shutdown
 - User sign on (failed and successful) and sign off
 - Configuration changes
 - Account creation, modification, or deletion
 - Modifications of privileges and access controls
 - System alerts and error messages
 - (4) Type of event, date, time, user identification, and IP address or other machine identifiers must be recorded for each logged transaction where technically and operationally feasible.
 - (5) Sensitive information, such as passwords and actual system data, must not be stored in

the logs.

- b) Periodic reviews of audit logs will be conducted by the Entity Information Security Officer or other designated personnel.
- c) Only designated personnel are allowed to have access to the audit logs.
- d) Audit trail files and reviews are to be retained in accordance with the entity retention policies.

5) ROLES & RESPONSIBILITIES:

- a) Information Owners are responsible for ensuring that audit trails are implemented and maintained for their resources.
- b) Custodians are responsible for assisting information owners with implementing and maintaining audit trails for the resources for which they are responsible. Custodians must regularly review audit trails in a timely manner.
- c) Supervisors are responsible for assisting the Entity Information Security Officer in reconciling audit trail anomalies.
- d) The Entity Information Security Officer is responsible for periodically reviewing audit trails for all systems to ensure compliance with this policy.
- e) Information Users are responsible for understanding and acknowledging that their use of UNC SOM systems may be logged and audited.

6) DEFINITIONS:

- a) Audit Trail -In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- b) Custodian - The custodian of information is generally responsible for the processing and storage of the information. The custodian is responsible for the administration of controls as specified by the owner.
- c) Information Owner - The owner of a collection of information is usually the manager responsible for the creation of that information or the primary user of that information. This role often corresponds with the management of an organizational unit. In this context, ownership does not signify proprietary interest, and ownership may be shared. The owner may delegate ownership responsibilities to another individual by completing the UNC SOM Information Owner Delegation Form.
- d) Security Incident -Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies

- 7) **ENFORCEMENT:** Failure to comply with Information Security Policies and Standards by employees, medical staff, volunteers, and outside affiliates may result in disciplinary action up to and including dismissal in accordance with applicable UNC SOM procedures or University procedures, or, in the case of outside affiliates, termination of the affiliation. Failure to comply with Information Security Policies and Standards by students may constitute grounds for corrective action in accordance with UNC SOM or University procedures. Further, penalties associated with state and federal laws may apply.

Authorship and Review

A subcommittee of the School of Medicine's HIPAA Security Team developed this policy. Questions, comments, or concerns regarding this policy should be directed to the School of Medicine's HIPAA Security Officer. This policy should be reviewed on an annual basis and all feedback provided on this policy will be considered during that review.

REVISION HISTORY: None

Approved by the HIPAA Planning and Oversight Council (HPOC): September 26, 2006.