Auditing and Accountability Policy

- Date of Issue April 2015
- Date of Review
- Purpose

The purpose of this Auditing and Accountability Policy is to define a consistent set of records collected from across the organization. This will enable quick response and handling of potential incidents. Without defined auditing requirements it is impossible to properly guard against advanced persistent threats, because evidence may not be gathered in a structured way. Consistent auditing records are the best defense in a long-term security plan.

- Scope;
This policy will apply to all of Mount Sinai Health System and its associated entities.

- Roles and responsibilities;
  o Management will:
    o Oversee implementation of this policy.
    o Ensure that exceptions to this policy are documented with Information Technology Security.
    o Provide training, in conjunction with Information Technology Security, to their constituents.
  o Information Technology Security will:
    o Maintain this policy in accordance with NIST guidelines to benefit the Mount Sinai Health System.
    o Review the policy, its articles and procedures annually or as is deemed necessary.
    o Support training activities having to do with this policy.
  o Application Owners will:
    o Establish classifications (PHI/PII) of data stored, processed or moved through systems.
    o Ensure that data handling controls are implemented and followed.
  o Authorized Users will:
    o Only access authorized systems and data.
    o Only assume privileges for which they are authorized.
    o Protect the systems, or information contained on systems, at the level in which it has been classified.
    o Share access to the system, or information contained within, with only authorized personnel.
    o Report any suspected, or actual, un-authorized access to their management team.
- Reference
  MSH HIPAA ACS-SMP.4.1
  CHP Security HS-005.3 / HS-001.4
  PCI DSS 3.0

- Policy

All electronic devices that reside on the Mount Sinai Health System network should have auditing turned on.

Mount Sinai Health System issued desktops and laptops have audit records that are generated and can be examined in the event of an incident.

At a minimum, all Mount Sinai Health System electronic devices that support auditing functions should record the items listed in the Auditing and Accountability Guidelines.

Mount Sinai Health System server's audit logs are not centrally managed. They are controlled by their owning entities who report suspicious log entries to IT Security using the Log Reporting Template packaged with this policy.

The Mount Sinai Health System defines audit failure events requiring real-time alerts in the Auditing and Accountability Guidelines. If an auditing failure occurs on a server the owning entity will be notified so that the issue can be remediated.

The Mount Sinai Health System requires audit logs for server systems to be checked for unauthorized logon attempts and escalation of privilege at least once per month. Indications of unusual activity should be reported to management for remediation using the Audit and Accountability Log Reporting Template. Records of these checks should be retained for one calendar year beyond the date of creation using the Audit and Accountability Log Template. (i.e. records for Feb 2014 should be retained through 2015.)

The Mount Sinai Health System reviews and/or updates the list of organization defined auditable events annually. Any changes, additions or subtractions to the list are notated in the Auditing and Accountability Guidelines.

The Mount Sinai Health System adjusts the level of audit review and analysis within the managed information systems when there is a change in the risk associated with a given system or situation.

Mount Sinai Health System allocates audit record storage capacity on hard drives belonging to servers to ensure logs can be accessed on demand. If audit logging exceeds that server’s log capacity, the system may be flagged for more space temporarily and monitored to determine the cause. The system can then
be assessed to decide if a permanent change in log size is necessary or if the auditing settings for that system must be altered.

Servers at the Mount Sinai Health System cannot be shut down in the event of an audit failure. This is due to the nature of applications interoperability as unplanned server shutdowns may result in an adverse effect on patient care. Acceptable ways for server owners to mitigate this risk are outlined in the Auditing and Accountability Guidelines.

At least annually the Audit and Accountability policy will be reviewed and updated by management to ensure its continued effectiveness. Otherwise, in the event that significant regulatory change occurs, the policy will be reviewed and updated as needed to ensure compliance.