STANDARD

1) Syslogs, event logs and other system logs should be kept online for a minimum of 4 weeks. Archives of logs should be kept for at least 18 months. If a violation or breach of confidentiality or security is verified, the logs relating to the incident will be maintained for a minimum of 6 years.

2) Requirements for audit logs for access to Restricted Information.

   Below, individual means patient, human research subject, employee, student or other individuals for whom audit logs will be generated. As per HS Policy 9462, there must be audit logs for access to Protected Health Information (PHI) and there should be audit logs for access to non-PHI Restricted Information.

   a. Audit records must be generated for view access, as well as for changes.

   b. Audit records must contain the following data elements:

      i. Date and time of access. Must have time resolution to the second.

      ii. User ID

      iii. User name

      iv. Name of the individual whose Restricted Information is being accessed

      v. Unique identifier for the individual. For patients, this should be the Medical Record Number (MRN).

      vi. IP address and/or Computer name of the user accessing the information

      vii. Information accessed. This can be a screen name, function name or something that explains what the user was doing. If internal codes are used, then a list of descriptions for the codes must be provided.

      viii. Any other information that helps explain the user's activity such as document or report ID numbers, accession numbers, etc.

   c. Audit records should also be generated for the user activities below. (These activities are not necessarily associated with any particular patient so usually need to be retrieved by searches on User ID.)

      i. User login and logout times

      ii. Session auto-logout for a user after a period of inactivity

      iii. Printing and/or export of data

      iv. Launching other applications

   d. Audit reports

      i. The audit records for a user or an individual or all access in a specified time period must be exportable as an Excel spreadsheet or .csv file.

ii. Standard by-user or by-individual reports should be developed.

iii. Application administrators must provide audit logs when requested by the Office of Compliance Services.

iv. If only the vendor will be able to extract audit log data and create reports, the request process must be documented and approved.

v. It should be possible to extract audit records by an automatic process to aid in any future central consolidation of audit records.

e. Audit log security

i. Access to audit logs must be restricted to the minimum necessary number of administrators.

ii. Audit logs must never be changed. There should be security controls in place to prevent changes.

f. Audit log retention

i. For patient information, HIPAA requires retention of audit logs for 6 years. Adequate store space must be allocated to ensure logs are not overwritten or lost.

ii. For non-PHI Restricted Information, consult with the Office of Compliance Service.

g. Time synchronization. Servers that generate audit logs must use time synchronization services such as NTP to ensure the date/time stamps on audit records can be reconciled with other events.

QUESTIONS

1) To learn more about how to implement audit and system monitoring logs, please contact your IT support group.
2) For questions on this Standard, please contact the Office of Compliance Services – Privacy and Information Security (PrivacyInfoSec@mednet.ucla.edu).

REFERENCES

HS Policy No. 9462, "*Privacy and Information Security Auditing and Monitoring*"

CONTACT

Chief Compliance Security Officer, Office of Compliance Services

REVISION HISTORY

Created Date: May 26, 2018

Revised: October 9, 2018