Policy Number: HC-25	Page: 1	Of: 2
Title: Audit Control and Activity Review		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/21/2021		
Reviewer/Job Title: Director of Operations		

(A) AUDIT CONTROL AND ACTIVITY REVIEW
System capabilities for maintaining audit trails of system use shall be enabled to permit forensic analysis and periodic activity reviews. Periodic activity reviews should be conducted to identify inappropriate activity so that appropriate corrective action is possible.

Audience

Hipaa privacy/security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164

164.312(b)

164.308(a)(1)

164.308(a)(5) Log-in Monitoring

1) **System Activity Logs**. Activity logs shall be enabled at the following levels:
   a) **Operating System** (Windows Server 2007): Audit Policy should be set to log logon events, account management events, policy changes, and system events.
   b) **Firewall Hardware and Software**: Logs should be enabled to track inbound and outbound activity, including internet access by individual.
   c) **Application Software Logging**: All software which stores data on individuals served shall have audit trail capabilities. Logs should be enabled in application software such as clinical record software, billing software, or information systems which store information regarding Individuals being served.
   2) **Security on Logs**. Appropriate security features and passwords should be used at all levels above to permit log file access only by the HIPAA Security Officer and/or an individual designated by him/her.
3) **Quarterly Audit of PHI Access**. A review of system activity will be conducted on at least a quarterly basis. The HIPAA Security Officer shall design an audit strategy to

identify probable or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:

a) Access by individuals at unusual hours.
b) Higher access/usage levels than normal.
c) Accesses to records of relatives of celebrities, celebrities' children or employees.
d) Unauthorized changes to security settings.
e) Web sites viewed by employees to verify that they are work related.
f) Outside probe attempts and/or accesses via the internet connection.
g) Other Unusual patterns of activity.

4) **System Activity Review**. In a manner determined by the Information System Officer, he or she will monitor system activity to detect suspicious or unusual system activity.
5) **Corrective Action.** The HIPAA Security Officer will initiate corrective action, in conjunction with other members of the management staff, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
6) **Purge of Log files**. System Log files which grow large may be purged under the direction of the HIPAA Security Officer.
7) **Annual Policy Review**. Annual attention should be given this policy regarding audit controls, as the threat level varies and the cost of monitoring tools changes.