POLICY INFORMATION

Document # **6000**	Title: **Audit Controls**	Original Effective Date: **9/7/2016**
Safeguard: **Security- Technical**	Approved by: **Dean Beth E. Foley**	Review Date: **09/29/2017** **10/09/2019**

I. POLICY STATEMENT

It is the objective of CEHS to ensure that all systems containing ePHI are identified, monitored and reviewed using audit controls that record and examine activity.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

Any CEHS HCC that creates, processes, transmits, or stores ePHI shall have implemented hardware, software and/or mechanisms to record and examine activity in the system(s) that contain or use EPHI. Audit controls include:

1. **Audit Procedures:** The CEHS Security Officer and applicable System Administrator(s) will identify and document all systems that contain ePHI. Documented audit trails will be maintained and regularly reviewed to determine sensitive events, and analyze out-of-tolerance conditions that indicate possible fraudulent and/or impermissible use of the system, such as repeated unsuccessful logons and access attempts over a series of days or during off hours. The Security Officer and applicable system administrator(s) will establish and document appropriate procedures to aggregate, manage and review auditing capabilities, audit logs and event reporting for monitoring. Minimum requirements are:
    A. System and user actions to be captured.
    B. Data retention.
    C. Methods for capture, storage and review.
    D. Frequency of reviews.
    E. Assignment of responsibilities.
    F. Confidential information authentication.

2. **Auditing Capabilities Enabled:** Event reporting capabilities shall be enabled for system and user activity.

3. **Audit Log Review:** The Security Officer (or designee) will perform audit log reviews on a regular basis. At minimum, the following should be part of the review process:
    A. Mechanisms must be established so that systems are not halted when logs become full and that logging can continue with little or no disruption.
    B. Review sufficient sampling of records or file access.
    C. Review user login information including login successes and failures.
    D. Review of whether security incidents were reported and proper follow up was performed.
    E. Ensure that all user access lists are current and all unauthorized access capabilities have been removed.
    F. Review to determine if the policies and procedures associated with access authorization are being followed.

4. **Audit Trails:** CEHS System administrators must include the following in audit logs:
    A. Individual user ID.
    B. Specific capabilities accessed and failures thereof (such as software, commands or files).
    C. Dates and times of access.

5. **Event Reporting:** Event reporting may be derived from various sources such as application reports, firewall or other network layer logs, domain logs, and operating system logs. Events should be promptly reported to the Security Officer, including items such as the following:
    A. Access at unusual times and/or from unusual places.
    B. Multiple failed logons.
    C. Unusual and/or saturated attempts to access system resources.

6. **Notification of Abnormal Conditions**: Systems and applications that create, process, transmit, or store ePHI shall develop, implement, and maintain alarms for reporting and providing signals of abnormal conditions. Regularly scheduled security audits or reviews will be performed by the Security Officer (or designee) to control and monitor reporting of operational irregularities.

7. **Integrity:** Systems and applications that create, process, transmit, or store confidential information shall protect against unauthorized alteration or destruction at all times and ensure the validity of the stored data.

8. **Confidential Information Authentication**: Systems and applications managing ePHI shall have a unique user identification and authentication mechanism for providing access to and maintenance of EPHI.

9. **Information Systems Activity Review:** CEHS Security Officer shall have regular review of information system activity, such as audit logs, access reports and security incident reports for all systems that create, process, transmit, or store ePHI.

10. **Audit Log Retention and Protection:** All systems that create, process, transmit, or store ePHI must include:
    A. Configuration settings must be documented and compared to actual setting to ensure unauthorized changes to logs have not occurred.
    B. Establish separation of duties between personnel who administer the access control function, those who perform the logging of events, and those who review the logs.
    C. Controls must be in place to protect against unauthorized changes and operational problems such as: the logging feature being de-activated, alterations to the message types being recorded log files being edited or deleted, and protection of log file media.
    D. Mechanisms must be established so that systems are not halted when logs become full and that logging continues with little or no disruptions.
    E. Audit logs should be readily available for at least a year and retained for at least six years. Only authorized access to logs is permitted. All accesses, reviews and archiving should be recorded.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100

45 CFR §164.312(b)