INFORMATION TECHNOLOGY AUDIT
& ACCOUNTABILITY

Policy: The University shall create and implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

<u>Rationale:</u> The Information Technology Audit and Accountability Policy addresses requirements to implement procedures to regularly review records of information system activity.

POLICY STATEMENT:

The purpose of this policy is to comply with federal regulation requirements to perform system activity review. Audits and logging enable identification of risk-impacting changes to organizational information systems and the environments in which the systems operate. This activity verifies that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.

<u>Compliance</u>

1. This policy applies to all forms of ePHI.

2. IT resources that store, access or transmit ePHI shall electronically log activity into a central location and conform to standards established by the Information Security Office.

3. Logging shall include system, application, database, and file activity whenever available or deemed necessary.

4. Logging shall include creation, access, modification and deletion activity.

5. Log data shall be retained electronically in accordance with State of Connecticut retention schedules.

6. HIPAA-Covered Components are responsible for developing and implementing procedures for logging activity.

7. IT resources and log files shall be periodically examined for access control discrepancies, breaches and policy violations.

8. System activity review cycles shall include review of audit logs, access reports and security incident tracking reports, and shall occur at least once per month.

Implementation

1. HIPAA-Covered Components are responsible for developing process for review of collected audit logs

2. HIPAA-Covered Components should utilize any published University of Connecticut Information Security Office standards for log collection.

Reference: 45 CFR 164.308