Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #14

Audit Control Procedure

Last Revised: 3/15/2005	*Approved: 12/12/2005*

Scope of Procedure

The scope of this Policy covers the hardware, software and/or procedural mechanisms that will be implemented by WU Business Units to record and examine activity in information systems that contain or use EPHI.

Procedure

1) Audit Control Mechanisms

a) WU HIPAA Security Policy requires that each Business Unit with systems containing medium and high risk EPHI must utilize a mechanism to log and store system activity. The logs **must** include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs **may** include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity. A schedule of review of system audit logs must be implemented. (See HIPAA Security Policy #2 - Security Management).

Audit Control Mechanisms:

- The VMS Alphserver Cluster contains several access logs to accomplish system access review: Operator Log, Monthly Accounting Summary and Accounting Log Utility
- Windows Servers contain Event Logs that document Application, Security and System events and are suitable for access review

b) Implementation of an audit control mechanism for systems containing low risk EPHI is not required.

2) Audit Control and Review Plan

- An Audit Control and Review Plan must be developed by each Business Unit and approved by the HIPAA Security Office. If the Business Unit's EPHI inventory changes, its Audit Control and Review Plan must be reevaluated and resubmitted to the HIPAA Security Office.

- Audit Control and Review Plan
    - Platform: VMS Alphaserver Cluster - Billing, Transcription, and Outcomes Systems
        - Logs maintained and reviewed by System Manager with frequency:
            - Operator's Log
                - All events: authentication, security, etc.
                - Review Frequency: daily
            - Monthly Accounting Summary
                - Summarizes all user technical activity by username
                - Review Frequency: monthly
            - Accounting Log
                - Detailed, technical session by session user log
                - Review Frequency: as needed, after Monthly Accounting Summary review
    - Windows Servers - (Planned) Billing, Transcription, Outcomes Systems
        - Logs maintained and reviewed by System Manager with frequency:
            - Event Viewer
                - Application Error Records
                - Security Audit Records
                - System Error Records
                - Review Frequency: daily