Oklahoma State University

Title: Audit Controls	Policy #: SEC-13.01
Category: HIPAA Compliance	Authority: 45 CFR § HIPAA SECTION: 164.312(b)
Standard: Access Controls	Responsibility: Health Care Components
Effective Date: 4/20/2005	Page 1 of 2
Approved By: OSU Legal Counsel	Revised: 7/1/2013

PURPOSE:

To identify mechanisms that record and examine activity in information systems that contain or use ePHI.

POLICY:

OSU will implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. *§164.312(b)*

Activity in information systems may be audited using the following procedures.

PROCEDURE:

1. Network services
    a. Review firewall logs
2. Servers
    a. Review various server logs
    b. EMR server shows administrator logins and log-in attempts.
    c. Vulnerability testing done annually and as needed periodically
3. Software
    a. Practice Management
    b. Electronic Medical Record
    c. Document Imaging System
4. Any screen where a user can change data in Practice Management, EHR or Document Imaging may be audited by the HIPAA Compliance Office or IT or other designee. This audit displays what the previous data was, what it was changed to, when it was changed, and the user id of who changed the data. The data may also show who has accessed, viewed, searched, added, updated, and deleted any records.
    a. Random Audits will be conducted on no less than a monthly basis, or as the need requires, whichever is of greatest frequency.
        1. Part of the audit will include verifying terminated employees access has been correctly removed from the various systems; and
        2. Current users are not accessing records outside of the scope of their respective job duties; and
        3. Checking to see if users have a high frequency of invalid login attempts

Oklahoma State University

Title: Audit Controls	Policy #: SEC-13.01
Category: HIPAA Compliance	Authority: 45 CFR § HIPAA SECTION: 164.312(b)
Standard: Access Controls	Responsibility: Health Care Components
Effective Date: 4/20/2005	Page 2 of 2
Approved By: OSU Legal Counsel	Revised: 7/1/2013

  b. If an audit trail outside of the scope listed above is needed, this may be requested of the Vendor.

5. Equipment (computers)
  a. The IT department can perform periodic spot check audit/scans on local drives to verify that storage of data files containing ePHI does not exist on the local drives of workstations.

6. Sanctions – Any use other than the intended that is found while auditing may leave the user responsible subject to OSU Sanctions and/or reporting to Law Enforcement or other governing bodies dependent on the findings of the audit(s).