Oklahoma State University

Title: Mechanism to Authenticate ePHI	**Policy #: SEC-14.01**
Category: HIPAA Compliance	**Authority: 45 CFR § 164.312(c)(2)** **HIPAA SECTION:**
Standard: Integrity	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 1 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

To guard against modifications or corruption to EPHI data

POLICY:

OSU will implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. *§164.312(c)(2)*

Each CHS employee is to know how to safely and securely handle and access EPHI. Each software system must have a mechanism to verify data integrity of electronically transmitted EPHI.

PROCEDURE:

OSU will utilize the security options of its various systems to lock down the user's ability to erroneously change or modify in any way. Outside of legitimate changes, the Audit logs will be used to track unwarranted changes to patient's records.

Practice Management

1. Data is encrypted for all PM transactions, internal and external.
2. The vendor has signed a business associate agreement agreeing to comply with the HIPAA Privacy and Security standards.

Electronic Medical Records

1. Data is encrypted for transmissions between client and server.
2. The vendor has signed a business associate agreement agreeing to comply with the HIPAA Privacy and Security standards.

Server

1. Communication between PM and EMR servers is in clear text but kept in a controlled internal environment.
2. To verify the integrity of this transmitted data, reports from applications are reviewed. These reports show any patient whose charges were not entered by CFS.

Interface

1. OSU servers sending data to outside parties via HL7 Interfaces or some other means will use secure transmission.
2. Data sent and received is thoroughly tested to ensure it arrives with the same data as it was sent, as to not mix-up patient information and ePHI.
3. Matching criteria between the various systems does vary, and therefore unlikely to change without completely vetting the change(s).

Local Computer

1. All documents, i.e. MS Word, MS Excel, containing ePHI created outside of the medical servers are to be stored on the user's network home drive only.

External

1. Anything transmitted externally, i.e. from clients to the server or from the server to clients, is encrypted.
2. For clearinghouse functions, refer to the Isolating Health Care Clearinghouse Functions policy.
3. All CHS employees who wish to access EMR and Practice Management remotely must do so via a VPN client. Procedures are defined in the Encryption and Decryption policy.

REFERENCE:

Isolating Health Care Clearinghouse Functions
Encryption and Decryption