Oklahoma State University

Title: Encryption	**Policy #: SEC–16.02**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.312(e)(2)(ii)**
Standard: Transmission Security	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Pages: Page 1 of 3**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

To ensure secured transmission of EPHI data

POLICY:

OSU will implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. *§164.312(e)(2)(ii)*

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:

Email

1. All external (outside OSU) email containing PHI will only be sent via OSU's Secure Email system, no exceptions.
2. No ePHI is to be stored in the email software system as a "contact" or within a "calendar" event or invite or within a "task".
3. All employees needing to send PHI via email are to receive training on the proper usage of the encryption portion before any sending via the encrypted method.
4. Employees who needlessly send email via the encrypted system may receive sanctions per OSU Sanction Policy.
5. Employees who send ePHI unencrypted may receive sanctions per OSU Sanction Policy.
6. The HIPAA Compliance Office and/or IT will periodically review the usage of the Secure Email System and the emails therein for auditing purposes in order to keep OSU's Patients information private and secure.

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.

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 network drive only. No storing of ePHI on a local hard drive is allowed.

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.

Laptops

The OSU in Tulsa Information Technology department will install encryption software on all laptops currently in use on the OSU CHS campus and at clinical locations. Once completed, the list will be provided to the OSU CHS HIPAA Compliance Office. Beginning FY14, laptops purchased for the use at OSU-CHS and at clinical locations will use hard drive encryption and not software encryption.

NOTE: The OSU in Tulsa Information Technology department will store software encryption keys in a secure network location. IT administrators are the only individuals who will have access to the software keys and will only be used to restore files.

Texting:

1. Any OSU employee that texts anyone else, and the text contains any form of PHI, must be encrypted with OSU's approved "texting" encryption software.
2. If no encryption software is available to the employee, then texting PHI is not allowed.

3. Any OSU employee who needlessly texts via the encrypted system may receive sanctions per OSU Sanction Policy.
4. Employees who text ePHI unencrypted may receive sanctions per OSU Sanction Policy.

Clearinghouse

1. All transactions that occur on the clearinghouse system are encrypted.
2. The database itself is encrypted.
3. All links to and from the clearinghouse system are encrypted via SSL certificates.
4. Any attempts to login to the system un-securely will automatically be redirected to the secure authentication mechanism before actually authenticating the login credentials.
5. Only authorized users will be allowed to login to the clearinghouse system.

REFERENCE:

Isolating Health Care Clearinghouse Functions
Encryption and Decryption
Sanctions