University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 9.6

Title:	**Transmission Security**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**04/05/05**
Applies:	**All UCD campuses**

Introduction

Purpose

This policy implements reasonable and appropriate technical security measures for all electronic Protected Health Information (ePHI) in transit, to guard against unauthorized access to and improper alteration or destruction of the ePHI.

Reference

45 C.F.R. § 164.312(a)(2)(iv)

45 C.F.R. § 164.312(e)

Applicability

This policy applies to ePHI that is transmitted over an electronic communications network (local area network, Internet connection, wireless, dial-up lines, high speed access, sending files, e-mail or facsimiles originating from computer based software applications). It is the responsibility of anyone who transmits or makes available for disclosure ePHI in any capacity at UCD to follow this policy.

Policy

The UCD Information Technology Services Department (ITS) shall put in place and shall maintain appropriate enterprise and network perimeter controls that will ensure the automatic protection of ePHI in transit.

Procedures

A. Transmission Security

1. Transmission security refers to the secure exchange and preservation of data over electronic communications networks.

2. Units that will transmit ePHI over an electronic communications network must first weigh the risk of unauthorized access to or modification of the ePHI during transmission. The unit must then implement a reasonable and appropriate transmission security measure to adequately address the risk to the ePHI.

3. When transmitting ePHI electronically, regardless of the transmission security measure being used, units must take reasonable precautions to ensure that the receiving party is who they claim to be, has a legitimate need for the ePHI requested, and is being sent only the minimum necessary ePHI when the purpose of the transmission is not for treatment, payment, or health care operations.

4. If ePHI must be transmitted over an electronic communications network and no transmission security is available please see the "Exceptions to Secure Transmission" section below.

5. UCD web sites containing ePHI that will be accessed from the Internet must be accessed via secure file transfer and remote login protocols.

6. EPHI transmitted via facsimile (fax) using computer-based programs to send or receive the ePHI shall comply with all technical transmission security measures.

B. Transmission Security Measures

If ePHI is being transmitted over an electronic communications network, a reasonable and appropriate transmission security measure must be implemented to adequately address the risk to the ePHI.

1. Encryption and Decryption

a. All transmissions of ePHI from UCD to a recipient outside the UCD network (e.g. over the Internet) must utilize an encryption mechanism between UCD and the receiving entity or the file, document, or folder containing the ePHI must be encrypted before transmission.

b. Files containing ePHI to be transferred across the Internet must be transferred using a secure medium, such as a secure file transfer protocol.

c. E-Mail messages containing ePHI intended to be transmitted outside the UCD network must be encrypted and transmitted using the approved

secure messaging product in use by UCD. See the Secure E-Mail Transmission policy.

2. Other Methods

As other transmission security measures are investigated and approved by ITS they will be added as options here. If a unit would like a use a security method other than encryption it must first receive written approval from the HIPAA Security Officer.

C. Integrity Controls

1. Units sending ePHI over an electronic communications network must implement transmission security measures to ensure that ePHI is not improperly modified during transmission.

2. EPHI integrity shall be sustained using approved mechanisms (e.g. checksums, hashing algorithms, electronic signatures and digital signatures) whenever available and feasible to protect against unauthorized alteration, tampering, corruption, or falsification of the ePHI.

D. Exceptions to Secure Transmission

1. Situations may arise when it is infeasible to comply with the above secure transmission controls. If this occurs, care should be taken that all possible methods have been investigated.

2. Permission for insecure transmission must be received in writing from the HIPAA Security Officer prior to the transmission.

3. After receiving permission for insecure transmission, units sending ePHI insecurely must make certain to minimize the ePHI sent and to redact any highly sensitive information if possible.