POLICY INFORMATION

Document # **9000**	Title: **Transmission Security**	Original Effective Date: **9/19/2016**
Safeguard: **Security- Technical**	Approved by: **Dean Beth E. Foley**	Date Reviewed: **9/29/2017** **10/09/19**

I. POLICY STATEMENT

It is the policy of CEHS to ensure that technical security measures are taken to guard against unauthorized access to confidential or sensitive information, including ePHI, that is being transmitted over an electronic communications network.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

The following **Integrity Controls** shall be implemented by CEHS IT before transmission occurs:

1. **Transmission Security Encryption:** Any confidential information transmitted to networks outside of CEHS HCCs shall have implemented encryption between the sending and receiving entity.
2. **Define and Document Process:** The Security Officer and CEHS IT System Administrator will establish and document a process that consists of the following:
    A. Authentication of the receiving entity or person.
    B. Level of encryption must comply with Utah State University's minimum accepted standard.
    C. Ensuring workforce members who transmit information are properly trained on the process involved.
    D. Ensuring workforce members must take reasonable precautions to authenticate the identity of the receiving party.
    E. Ensuring there is a legitimate need for transmittal of confidential information.
3. **Confidential Transmission using Email:** Transmission of confidential information via email shall only occur with approved and supported secure email solutions. The following safeguards must be utilized:
    A. The receiving entity has been authenticated.

B. The receiver is aware and prepared to receive the transmission.
C. Sender and receiver are able to implement an approved encryption mechanism.
D. All attachments containing confidential information are encrypted.
E. Emails containing ePHI must be sent from CEHS IT managed devices only.
F. Emails containing ePHI must include a privacy statement.
G. USU email accounts (@usu.edu) are the only accounts that USU business may be conducted with. Personal email accounts may not be used nor can usu.edu email be forwarded to a personal email account.

4. **Confidential Transmissions using Electronic Removable Media:** Transmitting confidential information via removable media including but not limited to CDs, DVDs, magnetic tape, removable hard drives, flash drives, and other hardware devices are prohibited. Files can be uploaded to the HIPAA approved Box folder.

Notification of Abnormal Conditions: Systems and applications that transmit confidential information shall have enabled alarms for reporting and providing signals of abnormal conditions that could adversely affect encryption of confidential information.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100

45 CFR §164.312(e)