Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # **9000**	Title: **Transmission Security**	Print Date: **9/06/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Technical**	Approved by: **Dean Beth E. Foley** DocuSigned by: Beth Foley 7AB6B86710B5491...	Date Approved: 9/19/2016

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:

1. **Transmission Security Encryption:** Any HCC that transmits confidential information to networks outside of CEHS shall have implemented encryption between the sending and receiving entity.
2. **Confidential Transmission to Outside Networks:** All confidential transmissions from CEHS to an outside network must utilize an encryption mechanism between the sending and receiving entity. The system administrator of such transmissions must establish 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. Workforce members must take reasonable precautions to ensure the identity of the receiving party.
    D. Ensure that 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.
4. **Confidential Transmissions using Electronic Removable Media:** Transmitting confidential information via removable media including CDs, DVDs, magnetic tape, removable hard drives, flash drives, and other hardware devices require the use of appropriate safeguards to ensure that such confidential information is protected against unauthorized use and disclosure. Such safeguards include:
   A. Authentication of the person or entity requesting the confidential information.
   B. Transmitting only the minimal amount of confidential information necessary to comply with the request or use.
   C. Storing and transporting media in a secure environment.
   D. Using an approved encryption mechanism.
5. **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

45 CFR §164.312(e)