Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # **5000**	Title: **Technical Access Controls**	Print Date: **8/15/2016**
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: 9/2/2016

I. POLICY STATEMENT

CEHS will implement reasonable and appropriate measures to (i) limit access to EPHI only to those persons that have been granted access rights based on their required functions and (ii) prevent those who have not been granted those rights from obtaining access to EPHI.

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 (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

1. **Unique User Identification**:
   Access to an information system requires the use of a unique user identifier in conjunction with an associated password or other type of authenticator that has been approved by CEHS. Two-step authentication must be used when accessing systems with EPHI. Unique User Identification is step one. Step two could include but is not limited to: DUO push identification method, strong password, PIN, token, or biometrics.

2. **Emergency Access Procedure:**
   For all systems that contain EPHI or sensitive information, an emergency access procedure must be in place. The HCC system administrator will work with the CEHS Security Officer to document the procedure for each system. The procedure will define who has access to the system and ensure the following:
   a. At least two individuals possess the highest access level with sufficient rights to add, remove, modify, backup and restore the data contained in the system.
   b. At least two individuals possess the highest access clearance for physical access to the console that manages the information.

   c. The conditions under which this emergency access procedure it to be implemented.

3. **Automatic Logoff:**
   When a device is unattended, automated security features and procedures will be employed to deter unauthorized access to EPHI, as follows:
   a. If the system has an automatic log off capability, then the feature will be enabled to terminate an electronic session after a predetermined time of inactivity (5 to 15 minutes). The inactivity time should be determined based on physical location of the device used to access the application, the nature of the application, and the user needs.
   b. If the system does not have an automatic logoff capability, then an electronic method will be employed to lock the application or device after a predetermined time of inactivity (e.g., password-enabled screensaver). The inactivity time should be determined based on physical location of the device used to access the application, the nature of the application, and the user needs.
   c. If the system cannot meet either of the requirements defined above in 3 (a) and (b), (e.g., due to technological limitations or because such security measures would impede necessary operations), then an exception must be obtained from the USU ISO Security Officer. If an exception is obtained, then users will procedurally logoff or lock the application or device or physically secure the device (e.g., in a locked room or cabinet) as necessary to deter unauthorized access whenever the device is left unattended.

4. **Encryption and Decryption:**
   It is the policy of CEHS that all devices containing EPHI will be encrypted. The following components must be implemented:
   a. Keys that are used to encrypt EPHI must be protected with the same care as the information itself.
   b. Any encryption application used must comply with current industry standards and/or NIST encryption standards, whichever standard is higher.
   c. Data encryption must take place before confidential or sensitive information, including EPHI, is placed on a public or wireless network for transmission.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR § 164.312(a)(2)(1)

45 CFR § 164.312(a)(2)(i), (ii), (iii), (iv)