POLICY INFORMATION

Document # **5000**	Title: **Technical Access Controls**	Original Effective Date: **8/15/2016**
Safeguard: **Security- Technical**	Approved by: **Dean Beth E. Foley**	Review Date: **09/22/2017** **10/4/2019**

I. POLICY STATEMENT

CEHS will implement reasonable and appropriate measures to (i) limit access to electronic Protected Health Information (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-factor authentication is the best practice for applications when accessing systems with ePHI, as applicable. Unique User I dentification is step one. Step two could include but is not limited to: DUO push identification method, strong password, PIN, token, or biometrics.

   Workforce member responsibility:
   Password Requirements:
   - Users must maintain strong passwords that are not easily guessed by individual or automated guessing, and are not easily cracked by hackers.
   - Passwords must be twelve or more characters long. They should contain a combination of upper and lower case letters, numbers and when possible, special characters such as !@_ or &.

Password Guidelines:

- Never give passwords to anyone. Users are responsible for all activity that occurs from their account.
- Users should choose passwords that are easily remembered by them, but not obvious to anyone else.
- Passwords should not be written down, posted next to computers or sent in an email message.
- Passwords must be unique – not used in another application or login.
- Work-related login and passwords should never be saved in an unsecure manner such as in browsers, such as Firefox.
- Passwords that are a uncommon phrase or mix of words are more secure than single words.
- Passwords should be immediately changed if it is suspected to have been discovered.
- Users should test password selections if possible.

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 or their designee 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 Lock:**
   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 lock capability, the feature will be enabled to terminate an electronic session after a predetermined time of inactivity (5 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 lock capability, the user should insure that the system is locked or logged off.

   Workforce member responsibilities:

- Users should log off or power off computers whenever it will be left unattended and/or unsecured for any length of time.
- Inactivity times are set by CEHS IT and may not be altered by the user.

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.

   Workforce member responsibilities:
   - New devices should be taken to CEHS IT to insure it meets encryption and security standards.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100- Definitions

USU Policy 550: Appropriate Use of Computing, Networking, and Information Resources

45 CFR § 164.304

45 CFR § 164.312(a)(2)(1)

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