POLICY INFORMATION

Document # **500**	Title: **Information Access Management**	Original Effective Date: **9/7/2016**
Safeguard: **Security** **Administrative**	Approved by: **Dean Beth E. Foley**	Date Reviewed: **10/6/2017** **10/2/19**

I. POLICY STATEMENT

It is the policy of CEHS to establish and maintain a formal documented information access management process. Access to CEHS information systems containing ePHI must be authorized only for properly trained workforce members who have a need for specific information in order to accomplish a legitimate task. Access must not be allowed until properly authorized. Access should be restricted to the minimum necessary for the workforce member to complete their job duties. All access must be regularly reviewed and revised as necessary.

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

Access Authorization, Establishment and Modification (Addressable): The Security Officer will develop, implement and maintain a formal documented process for granting and authorizing appropriate access to CEHS information systems. The documented process for granting access to systems that contain electronic Protected Health Information (ePHI) should, at a minimum, include:

a. A procedure for granting access to CEHS information systems containing ePHI that includes establishing, documenting and reviewing different levels of access to ePHI systems

b. A procedure for modifying workforce members access privileges to CEHS information systems containing ePHI.
c. A procedure for revoking access to systems containing ePHI.
d. When appropriate, security controls or methods that allow access to be established to CEHS information systems containing ePHI must include, at a minimum:
    i. Unique user identifiers that enable individual users to be uniquely identified. User ID's common or shared identifiers must not be used to gain access to CEHS information systems containing ePHI. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to CEHS information systems not containing ePHI. However, this should be a last resort when there are no other feasible alternatives. Further, anytime shared identifiers are used, the system and/or applicable administrators and data owners must have a procedure of tracking the individuals that are aware of the shared identifiers/credentials. The shared identifiers/credentials must be changed promptly anytime an individual with knowledge of the credentials and password transfers or is terminated from employment, or no longer needs access to the ePHI for any reason.
    ii. The prompt removal or disabling of access methods for persons and entities that no longer need access to CEHS ePHI.
    iii. All revisions to CEHS workforce member access rights must be tracked and logged.
    iv. This information must be securely maintained for a minimum of six years.

Responsibilities

1. The Security Officer and the system IT Administrator will define, document and authorize all access to information systems containing ePHI.
2. HCC workforce members must not willfully attempt to gain access to CEHS information systems for which they have not been given proper authorization.
3. HCC workforce members will not share their user id and login information with anyone and will not allow another individual to access ePHI systems under their credentials.
4. Appropriate CEHS information system owners/stewards must regularly review workforce member access rights to CEHS information systems containing ePHI to ensure that they are provided only to those who have a need for specific ePHI in order to accomplish a legitimate task. Such rights must be reviewed as necessary.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR 164.308(a)(4)(ii)(A)

45 CFR 164 308(a)(4)(ii)(B)