POLICY INFORMATION

Document # **500**	Title: **Information Access Management**	Print Date: **8/29/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7ABCBB86710B5191...	Date Approved: 9/7/2016

I. POLICY STATEMENT

It is the policy of CEHS to establish and maintain a formal documented information access management process that includes:

1. Access authorization procedures;
2. Access establishment and modification procedures; and
3. Procedures for the isolation of health care clearinghouse functions.

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 (Addressable): HCC must have a formal documented process for granting and authorizing appropriate access to CEHS information systems. The following safeguards must be implemented to satisfy the requirements of this standard:

1. HCC must have a formal documented process for granting access to CEHS information systems that contain ePHI. At a minimum, the process should include:
    a. Procedure for granting access to CEHS information systems containing ePHI.
    b. Procedure for tracking and logging authorization of access to CEHS information systems containing ePHI.
    c. Procedure for regularly reviewing and revising as necessary, authorization of access to CEHS containing ePHI.

2. HCC system administrator(s) will work with the CEHS Security Officer to define, document and authorize all access to CEHS information systems containing ePHI that is entrusted to them.

3. Access to CEHS information systems containing ePHI must be authorized only for HCC workforce members who have a need for specific information in order to accomplish a legitimate task. Access must not be allowed until properly authorized. All such access must be defined and documented as specified in the **Access Establishment and Modification** section below. Such access must also be regularly reviewed and revised as necessary.
4. HCC workforce members must not willfully attempt to gain access to CEHS information systems for which they have not been given proper authorization.

Access Establishment and Modification (Addressable): HCC's must have a formal documented process for establishing, documenting, reviewing and modifying access to CEHS information systems containing ePHI. The following standards must be implemented to satisfy the requirements of this standard:

1. CEHS HCC's must have a formal, documented process for establishing, documenting, reviewing and modifying access to CEHS information systems containing ePHI. At a minimum, the process must include:
    a. Procedure for establishing different levels of access to CEHS information systems containing ePHI.
    b. Procedure for documenting different access levels to CEHS information systems containing ePHI.
    c. Procedures for regularly reviewing workforce member access privileges to CEHS information systems containing ePHI.
    d. Procedure for modifying CEHS workforce member access privileges to CEHS information systems containing ePHI.
2. Only authorized and trained workforce members may access CEHS information systems containing ePHI. Such access must be established via a formal and documented process. At a minimum this process will include:
    a. Identification and definition of permitted access methods.
    b. Identification and definition of length of time that access will be granted.
    c. Procedure for both granting a workforce member an access method (e.g. password or token) and changing an existing access method.
    d. Procedure for managing access rights in a distributed and networked environment.
    e. Appropriate tracking and logging of activities by authorized workforce members on CEHS information systems that contain ePHI.
3. When appropriate, security controls or methods that allow access to be established to CEHS information systems containing ePHI must include, at a minimum:
    a. 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 by CEHS or the University, or no longer needs access to the ePHI for any reason.

   b. The prompt removal or disabling of access methods for persons and entities that no longer need access to CEHS ePHI.
   c. Verification that redundant user identifiers are not issues.

4. Access to CEHS information systems containing ePHI must be limited to CEHS workforce members who have a specific need to access ePHI in order to perform their job responsibilities.
5. Appropriate CEHS information system owners/stewards or their designated delegates 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.
6. All revisions to CEHS workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
   a. Date and time of revision.
   b. Identification of workforce member whose access is being revised.
   c. Brief descriptions of revised access right(s).
   d. Reason for revision.

   This information must be securely maintained.

V. ATTACHMENTS

N/A

VI. REFERENCES

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

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