POLICY INFORMATION

Document # **2000**	Title: **Facility Access Controls**	Print Date: **9/13/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Physical**	Approved by: **Dean Beth E. Foley** DocuSigned by: Beth Foley 7AB6B86710B5491...	Date Approved: 9/27/2016

I. POLICY STATEMENT

It is the policy of CEHS to establish and maintain facility access controls as a security standard for all work locations by limiting physical access to its information systems that contain ePHI by implementing reasonable and appropriate measures to allow only authorized person to access the facilities in which those information systems are housed.

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 implementation specifications are **ADDRESSABLE**. If a Healthcare Covered Component chooses not to implement any addressable safeguard, they will need to document what alternate means they are using and explain how these means meet compliance guidelines.

Contingency Operations-Emergency Access: Establish and implement as needed procedures that allow facility access in support of restoration of lost data in the event of an emergency or disaster.

a. HCC will identify for their area:
    i. The authority in charge and
    ii. The persons or classes of persons (e.g., workforce members, business associates, visitors) that may need facility access based on the nature and severity of an emergency or disaster.

b. Each Healthcare Covered Component will develop a process to regulate access in the event of an emergency or disaster including a manual authentication process,

if appropriate, to be implemented in the event that electronic means cannot be used.

c. Periodically test the emergency access process to substantiate that the workforce is aware of and can immediately respond in the event of an emergency or disaster. Testing dates and notes should be documented and retained for at least six years.
d. Each HCC will document the emergency access processes in the Facility Security Plan, as outlined in section 2 below.

1. **Facility Security Plan:** Each HCC will create and document a plan for their applicable area that are subject to this policy to safeguard the equipment therein from unauthorized physical access, tampering, and theft, and to support restoration of lost data.
    a. **Facilities Requiring a Security Plan.** HCC's will create a Facility Security Plan for each facility that houses information systems containing both ePHI and PHI, including:
        i. Server rooms or data centers (e.g., dedicated areas that house networked servers used for file storage, application hosting, data processing, etc.).
        ii. Peripheral equipment location (e.g., locations outside of data centers housing file and application servers, network switches, routers, etc.).
        iii. Offices that contain PHI, ePHI or other technical data that could be used to compromise the security information systems that maintain or are used to access ePHI.

    b. **Facility Security Plan Contents.** Each Facility Security Plan will address:
        i. Exterior Safeguards. Methods and procedures for safeguarding the exterior of buildings. Methods could include locks, cameras, fire doors, alarms or other access controls surrounding the premises as well as entrances and exits on the building.
        ii. Interior Safeguards. Methods and procedures for safeguarding the interior of buildings. Methods could include locks, alarms, or other access control authorizations and validations.
        iii. Equipment Safeguards. Procedures for safeguarding equipment contained within facilities and on premises. Methods could include isolation of equipment, controls to guard against theft, power surges and outages, fire and other types of damage.
        iv. Access Monitoring. Methods and procedures for collecting, retaining and reviewing facility access records such as facility access logs, and surveillance tapes.
    c. **Facility Security Plans Review.** Upon request, CEHS HIPAA Privacy/Security Officer(s), or Information Security Office may review the Facility Security Plan. The plan creator will review the Plan at least on an annual basis or when material modifications are made to the Plan.
    d. **Documentation Retention.** Each Facility Security Plan will be retained for a minimum of six years from the date when it was last in effect.

2. **Access Control and Validation Procedures:** Implement the following procedures to limit access to facilities or areas within a facility that are covered by this policy to authorized persons whose identities have been adequately validated.
    a. **Facility Control Management.** Each HCC will ensure:
        i. Proper procedures and documentation are in place to control and validate a person's access to areas are based on their role, including visitor control, and control of access to software programs.
        ii. Proper procedures and documentation are in place for administering the access control functions of the HCC (e.g., distribution, retrievals, and passcodes).
        iii. Proper procedures and documentation of facility access requests, approvals, and execution of access control mechanisms (e.g. distribution, retrieval of keys or prox cards).
        iv. Documentation of the above listed items shall be retained for a period of at least six years after the documented actions are no longer in place (e.g., six years following revocation of access granting rights or facility access rights).
        v. Access to equipment, rooms and other applicable areas will be granted only to those persons that have a legitimate need to access them because of their roles or job functions. Additionally, access rights will be revoked or modified upon termination or change in access needs.
        vi. Establish, in accordance with the Facility Security Plan, control mechanisms and/or authentication procedures to validate a person's identity and authority to access facilities based on current facility access rights. Visitors and workforce members whose roles do not require access to facilities or areas covered by this policy will be prohibited access unless they are authorized temporarily and accompanied by and appropriately authorized person.

The following implementation is **REQUIRED**:

1. **Maintenance Records -** Each HCC must implement procedures to document repairs and modifications to the physical components of a facility that are related to security (for example hardware, walls, doors, and locks). Required procedures are:
    a. Conduct and document analysis of existing physical security vulnerabilities.
    b. Maintain and document a current viable Disaster Recovery Plan and an Emergency Mode Operations plan.
    c. Create, implement and maintain a documented Facility Security Plan. The Facility Security Plan will include the following responsibilities:
        i. Create, implement and maintain physical controls on doors and cabinets using locks, video surveillance or other reasonable means of controls.
        ii. Create, implement and maintain a formal method for granting access to areas containing hardware, software and ePHI. This includes access controls on, but not limited to, maintenance personnel, vendors, and associates.

iii. Tracking and documenting all changes made to the environment, computer hardware and software. These changes include computer hardware and software maintenances, new hardware and software installations, hardware and software removal and any changes made to the physical environment. Documentation should include:
- Name and location of the facility location and the fixtures or equipment repaired or modified.
- Reason for the repair(s) or modification(s).
- The nature of what was repaired or modified.
- The name and affiliation of the business associate or other organization engaged to perform the work, if applicable.
- The name and affiliation of the technician or other professional who performed the work.
- The date(s) that the work was performed and completed.
- The manager who authorized the work.
- The manager who approved the completion of the work.

iv. Maintain a log of all access to sensitive areas including, but not limited to, computer room, data center, wiring closets and areas that contain or provide physical access to confidential or sensitive electronic information, including ePHI.

v. Create, implement and maintain a history file of all movement of equipment that contains PHI either into or out of a facility as well as documentation of how equipment was disposed of if appropriate.

d. Implement access control and validation procedures to control and validate a person access to sensitive areas based on their roles or function. This would include:
   i. Proper identification of person or persons being granted physical access to a facility or site. Such access authorization must be established and documented by the HCC.
   ii. Issue accurate identification badges that include the identification of the person, their approved areas of access and an expiration date if applicable.
   iii. Monitor, maintain and document a record of all access authorizations issued.
   iv. Update access should the person's role, responsibility or position change.
   v. Revoke the authorization in a timely manner when access is no longer needed.

e. Create procedures to ensure that all physical access controls are reviewed, tested and revised on a regular basis.

2. **Updating Physical Access Controls -** HCC will update the Facility Access Controls programs, as appropriate, to reflect any material changes in the procedures.

3. **Documentation of Access Controls -**
    a. Each HCC will document the Access Control programs utilized by its workforce members.
    b. Each HCC will retain for six years from the date the document was created all Access Controls related documentation, including without limitation:
        i. Access Control list of individuals who accessed each area, and
        ii. All written materials used for CEHS Access controls.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR § 164.310(a)