Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # **2000**	Title: **Facility Access Controls**	Original Effective Date: **9/13/2016**
Safeguard: **Security- Physical**	Approved by: **Dean Beth E. Foley**	Review Date: **10/20/2017** **03/08/2019**

I. POLICY STATEMENT

It is the policy of CEHS to establish and maintain facility access controls for all HIPAA 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 physically located.

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

1. **Facility Security Plan:** The Compliance Office will work with representatives in each applicable building to create and document a plan for each area that is subject to this policy to safeguard the equipment therein from unauthorized physical access, tampering, and theft, and to support restoration of lost data.

    a. **Areas Requiring A Facility Security Plan.** A Facility Security Plan will be created and maintained for each facility that houses information systems containing 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, labs and medical records rooms that contain PHI or other 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 prox access logs, and surveillance video.

c. **Facility Security Plans Review.** The plan will be reviewed at minimum, 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** will ensure:

   i. Proper procedures and documentation are in place to control and validate that a person's access to areas are based on their role, including visitor control in HIPAA areas, 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 (6) 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. 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 shall be established. 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 –** The Compliance Office will work with USU Facilities and each HCC to 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. 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.

    c. Maintain access control 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.

    d. 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.

    e. 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 identification badges that include the identification of the person, 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.

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

2. **Updating Physical Access Controls –** The Security Officer (or designee) will update the Facility Access Controls programs, as appropriate, to reflect any material changes in the procedures.

3. **Documentation of Access Controls -** Documentation will be retained for six years from the date the document was created all and shall include all written materials used for CEHS Access Controls.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100

45 CFR § 164.310(a)