POLICY INFORMATION

Document # **400**	Title: **Workforce Security**	Original Effective Date: **8/29/2016**
Safeguard: **Security Administrative**	Approved by: **Dean Beth E. Foley**	Date Reviewed: **10/6/2017** **9/30/19**

I. POLICY STATEMENT

PHI access by CEHS workforce members will be granted based upon the workforce members role within the HCC and will be restricted to the Minimum Necessary access for the workforce members to perform their job duties. Access will be monitored on a continual basis by the Compliance Officer or their designee. CEHS requires documentation detailing each workforce member's current role and responsibilities and the PHI access required for such role and responsibilities.

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. Authorization and /or Supervision - HCCs will implement procedures for the authorization and/or supervision of workforce members who work with confidential or sensitive electronic data, including PHI, or in locations where it could be accessed. The CEHS Compliance and IT Departments will be responsible for the security infrastructure, training, and oversight of computer and network maintenance personnel and will be accountable for:
    a. Developing and implementing security policies and procedures for CEHS.
    b. Training all members of the workforce on access methods to electronic systems and information.
    c. Identifying the persons or classes of persons in the workforce who need access to PHI.

Procedures include:

a. Procedures to ensure that access is only granted after receiving a written request from the supervisor and verification that the workforce member has a need for access and has completed all required training.
b. Procedures to ensure that all workforce members who do not need access to PHI or any area where such data might be accessed are not granted such authorization. The Minimum Necessary standard should be applied to all access requests.
c. Procedures to ensure that employees, students, contracted workforce members, patients and maintenance workers do not have unnecessary or inappropriate access to confidential or sensitive data, including PHI.
d. Procedures to ensure that appropriate supervision of workforce members when working on systems that contain confidential or sensitive data, including PHI.

2. Workforce Clearance Procedure – The Security Officer will implement procedures to determine that a workforce member is only given appropriate access to confidential or sensitive data, including PHI. In addition, The Security Officer will implement procedures to prevent individuals who should not have access from gaining access.

3. Termination Procedures
    a. Supervisors, Security Officer, and IT staff will ensure that access to PHI is terminated at the time of the workforce member's termination, and re-assessed for access limitations in the event of transfer from one job class to another.
    b. Supervisors will ensure that all access devices are returned by the workforce member at time of termination or transfer (if appropriate), and document this on the appropriate form.
    c. Supervisors will ensure that the Security Officer or designee and IT staff are informed of all staff terminations.
    d. In the event of an adverse termination, the Security Officer and IT staff should be notified prior to informing the workforce member, to ensure that information and systems are protected from potential retaliation.
    e. The Security Officer will ensure that the staff member's name is removed from internal e-mail lists and systems, access lists, and disable all access to the network.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100

164.308(a)(3)