POLICY INFORMATION

Document # **3000**	Title: **Workstation Use & Security**	Original Effective Date: **8/29/2016**
Safeguard: **Security- Physical**	Approved by: **Dean Beth E. Foley**	Date Reviewed: **9/15/2017** **03/08/2019**

I. POLICY STATEMENT

This policy shall establish minimum requirements for the implementation of physical safeguards for workstations that access electronic health information, and to restrict access to authorized users.

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 Components (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 components of CEHS.

IV. PROCEDURES TO IMPLEMENT

Logical and physical safeguards must be implemented for workstations that access or contain PHI to restrict access to authorized users. The safeguards include processes that define how workstations may be utilized for accessing information as well as physical attributes of the surroundings of workstations.

Workstation Use:

1. **Power-on and Screen Saver Passwords:**
    a. All workstation access must require user authentication.
    b. Password-protected screen savers should be invoked by users when workstations are left unattended to deter unauthorized users.
    c. Screen saver activation intervals should be short in length (e.g., 5 to 15 minutes). The time interval should be determined based upon the location and accessibility to the workstation.

2. **Password Standards:**
    a. Passwords must be unique and have a minimum of twelve characters with at least one alphabetic character, one numeric character and one symbol.

b. Passwords must be secured at all times. They must not be written and stored in an accessible location.
c. Passwords must not be shared under any circumstances.
d. Users are responsible for maintaining the confidentiality of their passwords. Any inappropriate use of a password will be the user's responsibility and could be subject to disciplinary actions and sanctions under the CEHS HIPAA Sanctions Policy 201.
e. Users are not allowed to use data under another person's account that has been logged into a system.
f. Users shall not observe the password entry of other users and shall make reasonable effort to prevent others from observing their password entry.

3. **Inactivity Timeouts and Manual Log-off:**
    a. Inactivity time-outs shall be enforced for workstations that access electronic Protected Health Information (ePHI). This time-out functionality should clear the workstation screen after a defined period of inactivity (e.g., 5 to 15 minutes).
    b. Users will log-off or place workstations in a secure or locked status whenever leaving it unattended.

4. **Off-site Computers:**
    a. Equipment containing confidential or sensitive electronic information, including electronic ePHI, should not be taken off-site without documented authorization. Where appropriate, equipment and /or software should be checked in and out.
    b. CEHS-owned equipment (including workstations) may only be used by the individuals approved to use it.

5. **Unauthorized Software:**
    a. Documented management approval is required for acquisition of all software.
    b. Prior to purchase an Inherent Risk Assessment must be performed on the system with the CEHS Information Technology (IT) Department.
    c. All software must be legally obtained, and reviewed by the CEHS IT Department, appropriately licensed and screened for viruses before installation.

6. **Acceptable Use:**
    a. Only USU/CEHS approved workstations should be used by workforce members for work-related purposes.
    b. Users should not save -information classified confidential, private, or otherwise considered sensitive or privileged information. Utah State University provides secure Box folders where this information can be stored safely and in accordance with USU policies.
    c. Users and HCCs should consult with the CEHS IT Department and the CEHS Compliance Office regarding questions about what kind of security and

safeguards are appropriate for the sensitive information they create, maintain, or transmit.

d. Workforce members are responsible for protecting the information resources at individual workstations and abiding by all Security Policies and Procedures that apply to their individual environment.
e. Workstations connected to critical business applications should be purchased with the help of the CEHS IT Department and the HCC unit's assigned system administrator. The workstations shall be tested prior to use, supported by effective maintenance arrangements and protected by appropriate physical controls.
f. Critical data must be backed up on a regular basis.

7. **Workstation Configurations:**
    a. The CEHS IT Department is responsible for defining base controls and configurations for workstation builds. CEHS system administrators will inventory each workstation/electronic device, and documentation of systems used on each workstation.
    b. Only authorized personnel (e.g., system administrator, CEHS IT) are permitted to perform workstation configurations.
    c. Workstation configurations or procedures should prevent users from:
        i. Installing unauthorized software.
        ii. Modifying system configuration files.
        iii. Modifying access control lists for systems files and other people's user files.
    d. Each workstation is required to be protected from malicious software by up-to-date anti-virus software or an appropriate and effective alternative. This shall be determined by the Director of Information Technology.

Workstation Security:

1. Workstations will be located in secure locations based on reasonableness of functions performed.
2. Workstations used infrequently will be located in a secure area or locked when not in use.
3. Doors leading into offices with desktop/laptops should always be locked when vacated.
4. Workstations that provide access to or use of sensitive information or information systems should not be located in publicly accessible areas.
    a. If a workstation must be located in a public area, physical and technical safeguards must be employed to protect against unauthorized access such as privacy screens, security locking cables or cages.
5. All workstation monitors are to be positioned in a way that prevents casual viewing by unauthorized users and the general public.
6. Users must ensure that all devices and media used at the workstation location are secured.

Monitoring and Auditing:

1. The CEHS Compliance Office and IT Department will monitor the Workstation Use and Security standards for compliance and changes, and update processes and procedures as necessary.
2. The workstation controls addressing the installation of unauthorized software will be monitored by the system administrator.
3. Violations will result in appropriate action based on the CEHS Sanctions Policy 201.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.310 (b), (c)

CEHS Privacy Policy 100

CEHS Sanctions Policy 201

USU Policy 311: Corrective Action

USU Policy 550: Appropriate Use of Computing, Networking, and Information Resources and

USU Policy 551: Computer Management