Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # **600**	Title: **Security and Awareness Training**	Print Date: **9/13/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 9/27/2016

I. POLICY STATEMENT

It is the policy of CEHS to establish and maintain a Security Awareness and Training program as a security standard for all members of its workforce.

This policy is applicable to all workforce members who are responsible for, access, or otherwise administer a healthcare computing system. A health care computing system is defined as a device or group of devices that store or access ePHI which is shared across the network and accessed by workforce members.

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

Security Awareness and Training Programs

CEHS Security Officer and Privacy officer must develop, implement, and regularly review a formal, documented program for providing appropriate security training and awareness to its workforce members. All health Care Components' workforce members must be provided with sufficient training and supporting reference materials to enable them to appropriately protect ePHI on CEHS information systems.

1. All new CEHS HCC workforce members must receive appropriate HIPAA and other applicable security training(s) within 30 days of hire and before being provided with access or accounts on CEHS information systems.
2. Existing workforce members must receive security training updates a minimum of once a year.

The Security Training programs will include the following topics:

1. Overview of CEHS's responsibilities for complying with federal security requirements.
2. Explanation of what constitutes Use and Disclosure of Protected Health Information (PHI).
3. Impact of CEHS's Security Policies and Procedures on workforce members' actions and interpersonal communications.
4. User education concerning protection form malicious software.
5. User education in importance of monitoring login success and failure and how to report discrepancies.
6. User education in password management.
7. Responsibilities' with respect to reporting violations of CEHS's Security Policies and Procedures.
8. A description of possible sanctions for failure to comply with CEHS's Security Policies and Procedures.
9. Periodic reminders of security issues and concerns.
10. Any State specific security laws, regulations, or issues, as applicable.

Documentation of Security Training:

1. CEHS components will document the security training programs conducted.
2. CEHS will retain documentation of training for six years for the date the documentation was created or the last effective date of the policy, including without limitation:
    a. Training session date and attendance list
    b. All training materials used for the training.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR 164.308(a)(5)(i)