Emma Eccles Jones College of Education & Human Services

POLICY INFORMATION

Document # **7000**	Title: **Information & Data Integrity**	Print Date: **10/24/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Technical**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 11/8/2016

I. POLICY STATEMENT

CEHS shall maintain the confidentiality, integrity and availability of all confidential information, including EPHI that is accessed, created, received, maintained, or transmitted within the Health Care Components (HCC).

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 (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 procedures are to be implemented in order to ensure the integrity of confidential information, including EPHI:

1. All CEHS HCC systems shall be evaluated, inventoried and documented by the Security Officer or designee. An inherent risk survey will be completed and will include assessing: network components, host systems, workstations and any other components that access, create, receive or transmit confidential information such as EPHI.
2. All information systems must be documented, tested and approved by the Security Officer prior to being placed in service within a HCC.
3. All IT resources that are used to access, create, receive, maintain or transmit confidential EPHI must possess adequate technical safeguards to protect the information that will be contained within it.
    A. Operating systems must be hardened before confidential information such as EPHI is placed on the workstation or server. Such hardening could include installation of a secure disk file system, closing of unnecessary access ports, and other steps as required to protect the information that will be contained on the system from unauthorized access, damage or deletion.

B. Network components must be configured to appropriately protect network traffic to these systems. Components include cabling and fiber, routers, firewalls, switches, etc.
C. All IT resources that will host or transmit confidential data and EPHI must include designating a HIPAA trained system administrator to ensure proper functioning of systems in and transmit securely.
D. Applications that contain confidential information such as EPHI must possess the following:
    i. Appropriate access controls such as unique user id, PIN's, password, or token access.
    ii. Appropriate logging and audit trail capabilities that recorded and log changes and deletions of the data.
    iii. Automatic log off where supported. Password protected screen savers should also be used.

4. All systems that access or contain confidential data such as EPHI must possess adequate protection from malicious software such as viruses, worms and other scripts or code that could damage the integrity of the data.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.312(c)