

POLICY INFORMATION

Document # 8000	Title: Person or Entity Authentication	Original Effective Date: 9/27/2016
Safeguard: Security- Technical	Approved by: Dean Beth E. Foley	Review Date: 09/29/2017 10/09/2019

I. POLICY STATEMENT

It is the policy of CEHS to ensure that all individuals or entities that access CEHS ePHI information systems have been appropriately authenticated.

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

In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to ePHI. In order to accomplish this, the Security Officer will implement the following procedures:

1. Workforce members seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as a unique user identification and password or biometric input to verify authenticity before being given access to information systems. In addition, whenever a person or entity is authorized to access such information, only the minimum necessary access needed to perform their designated function is to be authorized.
2. Workforce members seeking access to any network, system or application must not misrepresent themselves by using another person’s user ID and password, token or other authentication information.
3. Workforce members are not permitted to allow other persons or entities to use their unique user ID, password, token or other authentication information.
4. A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting ePHI.
5. When an external user accesses applications or data, authentication requires a user ID and stronger authentication mechanisms. External authentication is accomplished through

Emma Eccles Jones College of Education & Human Services

multiple/layers user IDs and passwords through virtual private network (VPN), and similarly secure authentication methods.

6. When any user is authorized to access confidential information, including ePHI, at the application level, the best practice is for that application to possess dual authentication capabilities, when available.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 100

45 CFR §164.312(d)