I. PURPOSE

This policy reflects East Carolina University’s commitment to ensure that all persons or entities seeking access to the university’s EPHI are appropriately authenticated before access is granted.

II. AUTHORIZATION AND ENFORCEMENT

Health Care component management and/or administrator(s) are responsible for monitoring and enforcing this policy, in consultation with the ECU IT Security Officer, ECU HIPAA Security Officer, and ECU HIPAA Privacy Officer.

III. POLICY

ECU Health Care Components must authenticate all persons or entities seeking access to the university’s EPHI before access is granted. ECU Health Care Components must use an appropriate and reasonable system(s) to ensure that only properly authenticated persons and entities access its EPHI.

IV. APPLICABILITY

This policy is applicable to all workforce members who are responsible for or otherwise administer a healthcare computing system. A healthcare computing system is defined as a device or group of devices that store EPHI that is accessed remotely by healthcare workers.
V. PROCEDURE

1. ECU Health Care Components must authenticate all persons or entities seeking access to the university’s EPHI before access is granted. Authentication may include, but is not limited to the following:

   • User name and password
   • Biometrics
   • Challenge and response mechanisms
   • Secure identification cards

VI. COORDINATING INSTRUCTIONS

1. All section policies, standards and procedures will be reviewed annually. Every section policy, standard and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other East Carolina University, University of North Carolina system, or state of North Carolina requirements may stipulate a longer retention period.