I. PURPOSE:
The purpose of this policy is to direct the business, healthcare, and academic components of the Affiliated Covered Entity (ACE) to create an environment and culture that enables the ACE to meet compliance with the standards of the HIPAA Security Rule.

II. POLICY:
All departments responsible for computer systems operated by the component organizations of the ACE will have adequate processes in place for authorizing Access to Electronic Protected Health Information in any form. These processes will include steps to assure that individuals granted Access to such information have a job related need for the Access; that the Access provided is limited to that needed to perform the person’s job functions; and that the Access is authorized by appropriate individuals before it is granted. Individuals granted Access to the computer systems and or databases of ACE must complete appropriate training on use of the systems and requirements for protection of the data, prior to being given such Access.

III. DEFINITIONS: See document “SECURITY POLICY GLOSSARY FOR DEFINITIONS OF SPECIAL TERMS (ACE-0999).

IV. PROCEDURES.
A. Standards:
1. The policies and procedures of the ACE relating to Information Security apply to all component organizations of the ACE and all members of the Workforce.
2. All computing resources shall be assigned a Resource Owner who is responsible for the Integrity, Confidentiality, and Security of the resource.
3. Access to any computer system or database containing Individually Identifiable Health Information is to controlled and protected by this policy.

B. Responsibilities:
1. Management of the component organizations comprising the ACE are responsible for assigning ownership of their respective computing resources, and for determining which resources contain Electronic Protected Health Information.
2. Each Resource Owner is responsible for granting Access to the resource only after the user has been appropriately identified, authorized and qualified for Access.
3. Department managers, or designated alternates, are responsible for authorizing Access requests for individuals in their groups. They are expected to sign such Authorizations only after consideration of the individual’s need for Access to the resource, and the scope of Access needed to perform their job duties.
4. Resource Owners are responsible for determining the applicable pre-qualifications for Access to the resources (e.g., training).
5. Individuals being granted Access to an ACE resource are required to sign for such Access, and to have that signature include their pledge to use the resource responsibly and to protect the Security of the Electronic Protected Health Information they utilize.
6. The Corporate Compliance Officer is responsible for establishing a program and schedule of reviews of the component organizations of the ACE for the compliance with this policy.
7. The Compliance Office and the Information Security Officials of the ACE are responsible for support of groups with questions relating to compliance with this policy.
8. The designated ACE Information Security Official has overall responsibility for maintaining this policy and these procedures.

V. RESOURCES:
A. Compliance Office
B. ACE Security Official (804) 828-1990
C. Information Security Contacts

VI. REFERENCES:
A. HIPAA: 45 C.F.R. §164.308 (a) (4) (i).
B. VCU Health Systems – Glossary of HIPAA Terms
C. VCU Health Systems Compliance Manual
D. Implementation Directive – ACE-0002

APPROVED:

Signature on File
Dr. Sheldon M. Retchin, M.D., M.S.P.H.