I. PURPOSE:
This policy relates to the establishment of Technical Safeguards (controls) in the form of policies and procedures that apply to Affiliated Covered Entity (ACE) Information Systems that create, receive, maintain, or transmit Electronic Protected Health Information. This policy also provides that these “technical” procedures serve to initiate specific directions and “gate keeping” rules designed to allow Access to Electronic Protected Health Information to only those individuals or software programs that have been granted Access rights, pursuant to the established Information Access Management policies and protocols (VCUHS Policy #1502 and #1503).

II. POLICY:
The ACE will apply reasonable and appropriate Access protocols, mechanisms, measures and guidelines to assure that only individuals granted Access rights to the organization’s Electronic Protected Health Information are able to Access this information.

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 resources containing Electronic Protected Health Information require a user to know, at minimum, a User ID and the associated, current password.
4. Individuals must be instructed to keep User IDs and passwords confidential, and to change passwords periodically.

B. Responsibilities:
1. Each Resource Owner shall assure that Access Control Lists are maintained noting the members of the Workforce authorized to Access the system or resource and shall assure that the systems limit Access to personnel on the list who are properly Authenticated to the system or resource each time.
2. Resource Owners shall implement the tightest password management capabilities available for their system / resource that are reasonable and appropriate. These guidelines shall include minimum password lengths, format of passwords, forced changes of passwords and auto-logout capabilities after periods of disuse.
3. Resource Owners shall utilize and monitor Access logs, failed login attempt reports, and shall follow-up on all reported incidents.
4. The Compliance Office, Information Security Officials, and Assurance Services shall Audit systems and databases, periodically, to assess the
degree to which the available Technical Safeguards (to access of the data) are being employed and the effectiveness of the safeguards.

IV. RESOURCES:
A. Compliance Office 

V. REFERENCES:
A. HIPAA: 45 C.F.R. §164.312 (a) (1).
B. VCU Health Systems – Glossary of HIPAA Terms (ACE-0999)
C. VCU Health Systems Compliance Manual
D. Implementation Directive – Policy ACE-0002

APPROVED:

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