I. PURPOSE:  
This policy is designed to prevent, detect, contain, and correct security violations.

II. POLICY:  
The Information Security Groups of the Affiliated Covered Entity (ACE), under the leadership of the designated Information Security Official for the ACE will:

1. Implement a comprehensive security management program for identifying and reducing reasonably anticipated adverse events that threaten the Integrity, Confidentiality, and Availability of Electronic Protected Health Information, and to prevent, detect, contain, and remediate compliance risk conditions.

2. Implement a risk management program that identifies and reduces factors that contribute to adverse events, unanticipated disclosures, or Threats to Electronic Protected Health Information caused by inappropriately designed or absent Security Measures, Security systems, or Administrative, Physical, and Technical Safeguards.

3. Establish an environment in which ACE leaders can identify and manage actual and potential risks to the Security, Integrity, Confidentiality, and Availability of Electronic Protected Health Information.

4. Recognize risks and reasonably anticipated events.

5. Initiate actions to reduce risks and mitigate resulting harm.


7. Establish and maintain reasonable and appropriate Security Measures and technologies.

8. Investigate factors that contribute to risk conditions, incidents, or violations of the ACE governance Security policies, or the Security Rule.

9. Assess current Security Rule compliance conditions throughout the ACE.

10. Improve risk management performance through the retirement of identified risks, and remediation of harm that may have been caused as a result of a risk or a violation of the Security Rule standards.

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

IV. PROCEDURES:
A. Standards:
1. Each component organization of the ACE will designate a primary Information Security contact.

2. All computing resources shall be assigned a Resource Owner who is responsible for the Integrity, Confidentiality, and Security of the resources.

3. All computer systems, databases, computers, portable data storage devices, PDAs, etc, containing Electronic Protected Health Information are covered by this policy.

4. Organization-specific policies and standard operating procedures will be implemented, for authorizing Access to Electronic Protected Health Information consistent with the applicable requirements of the Privacy Rule.
B. Responsibilities:
1. The designated ACE Information Security Official is responsible for the development and maintenance of this program and for measuring that the program is meeting its objectives.
2. The ACE Compliance Office is responsible for establishing a program of ongoing systems reviews and audits, of any and all places where the Electronic Protected Health Information is stored or used. Each such audit will be documented and any identified risks will be logged, classified, and tracked to retirement.
3. The ACE Information Security Official will establish a process for capturing reports of potential risks from any source and assign resources to proactively seek information about possible risks not yet encountered.
4. The ACE Information Security Official will review all requests for implementation of new systems, networks, and databases, that contain Electronic Protected Health Information, and no such changes or additions shall proceed without this approval.
5. The ACE Information Security Official shall maintain records of all attempted and/or successful Security breaches and shall report these to the Compliance Officer.
6. Resource Owners shall obtain the approval of the ACE Information Security Official before making any changes or taking any actions which could impact the Confidentiality, Integrity, or Availability of the Electronic Protected Health Information for which they are responsible.

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)(1)(i).
B. VCU Health Systems — Glossary of Security Policy Terms
C. ACE Overall Security Policy
D. VCU Health Systems Compliance Manual

APPROVED:

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