I. PURPOSE: Describes the Physical Safeguards that determine how Information Systems and Access to them, is secured from hazard, tampering, and Unauthorized Access. This includes the physical measures, software mechanisms, policies, and procedures that protect the electronic Information Systems and related building and equipment, from natural and environmental hazards, and unauthorized intrusion.

II. POLICY: Reasonable and appropriate Physical Safeguards will be employed across the Affiliated Covered Entity (ACE) to protect the Workstations used to Access and store Electronic Protected Health Information.

III. DEFINITIONS: See document “SECURITY POLICY GLOSSARY” FOR DEFINITIONS OF SPECIAL TERMS.

IV. PROCEDURES:
A. Standard:
   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. All devices displaying Electronic Protected Health Information shall be located so that only the operator of the device has the ability to view the information.
   4. Portable devices such as laptops and PDA’s must be equipped with software that does not allow an unintended user of the device to Access any stored Electronic Protected Health Information.
   5. As a general rule, Electronic Protected Health Information should NOT be stored on local Workstations, or copied to removable media such as tapes, diskettes or CD’s. The information should remain on centrally managed servers whenever possible.
   6. Devices in high traffic areas, or in areas not behind locked doors or normally manned, should be physically secured.

B. Responsibilities:
   1. Members of the Workforce are responsible for assuring that their use of Electronic Protected Health Information follows the ACE Policies and Procedures and their training related to the Confidentiality and privacy of patient data.
   2. The ACE Information Security Official will offer physical Security consulting for Workforce personnel requesting this and will be aware of the approved devices for physically securing Workstations.
   3. The owners of computing resources are responsible for assuring that servers, Workstations, etc., are reasonably secure, and that standard accepted safety practices are in place.
   4. The physical Security of the Workstations will be monitored via the following periodic processes: Compliance Office Audits, Security
Affiliated Covered Entity

HIPAA Security Rule Operational Policy

Official Audits, Fire Marshall Inspections, JCAHO certification reviews, etc.

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

VI. REFERENCES:
A. HIPAA: 45 C.F.R. §164.310(c).
B. VCU Health Systems — Glossary of HIPAA Terms
C. VCU Health Systems Compliance Manual
D. Implementation Directive – Policy SR-306a

APPROVED:

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