SUBJECT: Security Rule General Rules

POLICY NO.: ACE-0001

APPROVED DATE: 10/19/2005

EFFECTIVE DATE: 11/19/2005

REVIEWED DATE:

SUPERSEDES NO.: NEW

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 or exceed compliance with the standards of the HIPAA Security Rule by implementing policies and standard operating procedures that are designed to ensure the Confidentiality, Integrity and Availability of Electronic Protected Health Information (ePHI) that it creates, receives, maintains, or transmits. The policy also serves to protect the ePHI against any reasonably anticipated Threats or hazards to the Security or Integrity of the ePHI; as well as any reasonably anticipated uses or disclosures that are not permitted or required by the Privacy Rule. This policy also directs that a program be implemented to ensure Workforce compliance with the policies, procedures and Security Rule standards.

II. POLICY:
A. The ACE will ensure that the component organizations are reasonably and appropriately:
   1. Ensuring the Confidentiality, Integrity, and Availability of all Electronic Protected Health Information that the organizations create, receive, maintain, or transmit.
   2. Protecting against any reasonably anticipated Threats or hazards to the Security or Integrity of Electronic Protected Health Information.
   3. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law.

B. This policy directs that the following be implemented, at a minimum, in order for the ACE to comply with the Security Rule requirements:
   1. The ACE’s organizational components may use any Security Measures that allow for a “reasonable and appropriate” implementation of the standards and implementation specifications of the Security Rule.
   2. The ACE, in determining which Security Measures to use, considers the following factors:
      a) The size, complexity, and capabilities of its component organizations.
      b) The technical infrastructure, hardware, and software capabilities.
      c) The overall costs of the Security Measures.
      d) The probability and criticality of the potential risks to the Electronic Protected Health Information.

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

IV. RESOURCES:
A. Compliance Office
V. REFERENCES:
B. VCU Health Systems — Glossary of HIPAA Terms
C. VCU Health Systems Compliance Manual

APPROVED:

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