VCU Affiliated Covered Entity
HIPAA Security Rule Operational Policy

| | | | |
|---|---|---|---|
| SUBJECT: | | POLICY NO.: | ACE-0005 |
| | | APPROVED DATE | 10/19/2005 |
| | **Workforce Security** | EFFECTIVE DATE: | 11/19/2005 |
| | SR-308a3i | REVIEWED DATE: | |
| | | SUPERSEDES NO.: | NEW |

I. PURPOSE:
This policy is designed to ensure that all of the members of the component organizations Workforce have the appropriate level of Access to Electronic Protected Health Information, and that those members of the Workforce who are not authorized to access electronic information are prohibited from doing so.

II. POLICY:
A. Electronic Protected Health Information may only be accessed by those members of the Workforce who are authorized, based upon their role-based duties for such Access. The Affiliated Covered Entity (ACE) will implement all reasonable and appropriate Physical, Administrative and Technical Safeguards required to assure that Access to the Electronic Protected Health Information is appropriate.

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

IV. PROCEDURES:
A. Standards:
1. All computing resources shall be assigned a Resource Owner who is responsible for the Integrity, Confidentiality, and Security of the resource.
2. 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.
3. Approval for Access to the ACE computing resources shall require the signature of a member of the ACE Management (Approver) having appropriate understanding of the functions of the resource being requested and the role of the individual. All requests for Access must be documented.

B. This policy requires that the following be implemented:
1. Security Measures for Access Authorization and Authentication protocols based on an individual’s role and “position description” within the component organization with regard to the electronic object Access rights assigned and associated with a unique user profile and password.
2. Mechanisms are in place in which any individual’s Workstation or user profile is deactivated after a reasonable number of password violations, and further Access to electronic information is subsequently denied.
3. Procedural controls to recognize and acknowledge Access violations, and initiate investigations, appropriately.
4. Procedural controls to limit Access to removable data files and restrict this limited Access to authorized members of the Workforce.
5. Procedural controls for Access to data altering utilities is restricted to authorized personnel, and usage is closely monitored.
6. Procedural controls for Access to operations facilities and areas where Electronic Protected Health Information is stored, created, or transmitted, is restricted to only those individuals having Authenticated Authorization, based on their role (as defined in the organizational “position description”) and wherein leadership Authorization, for Access to specific facilities and “categories” of Electronic Protected Health Information is granted.

B. Responsibilities:

1. The computing Resource Owners are responsible for assuring that access categories are created (to the extent reasonable and appropriate) that model the individual role–based functions of those who will use the resource.
2. Approvers will determine the most appropriate Access category for an individual prior to approving the request for Access.
3. The computing Resource Owners shall implement and document the following:
   a) A mechanism that deactivates the User ID or Workstation after a designated number of failed login attempts.
   b) A process for monitoring Access violations, whether successful or not.
   c) Assurance that Access to systems tools (such as utilities) is tightly controlled and monitored
   d) Instructions to the authorized users regarding use of removable media for holding any electronic patient information, including the requirement that all such files be documented, inventoried, and tracked as to location and use.
4. Computer center managers are responsible for assuring that the areas, where the data are stored and are physically secured by use of limited Access Control Lists, monitoring, and physical locks.
5. All members of the Workforce who are granted Access to any ACE electronic protected health information are responsible for utilization of their Workstations, and use of the information for only their job functions and in a manner that protects the Security and Integrity of the information.

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)(2).
   B. VCUHS – Glossary of HIPAA Terms
   C. VCUHS Compliance Manual
   D. Implementation Directive – Policy SR-306a

APPROVED:

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