I. PURPOSE:
The purpose of this policy is to establish Security Incident Procedures detailing the process whereby the component organizations of the Affiliated Covered Entity (ACE) respond to Threats of unauthorized use, access or disclosure of Electronic Protected Health Information, and recover from any adverse effects of the events.

II. POLICY:
A. The component organizations of the ACE shall be prepared to quickly and effectively respond to any Threats to the Security of the Electronic Protected Health Information maintained by any of the component organizations of the ACE. Such response will first seek to avoid information loss, damage, or compromise; and further include processes to address recovery from intrusions, and follow-up actions to strengthen notice and avoidance capabilities in the future.

B. This policy addresses the HIPAA Regulation requirements under 45 CFR §164.308(a)(6)(i) that require the following Elements of Performance to be implemented:
1. Procedures to facilitate centralized reporting of information Security Incidents.
2. Procedures to coordinate the responses to known Security Incidents of a certain type, or affecting a certain technology or Malicious Software.
3. Initiate actions to provide technical assistance (as needed) to mitigate any harmful effects caused by a Security Incident; document the Security Incident and its outcome.
4. Recognize, acknowledge, respond to, and report any security related incident, event or technical Threat to Electronic Protected Health Information.
6. Investigate factors that contribute to the Security Incidents, and any violations of the ACE governance security policies, or the Security Rule.
7. Respond to Business Associate reported Security Incidents.
8. Distribute software Security Mechanisms, as considered reasonable and appropriate, to avert or contain Information Systems Security Threats and attacks to Electronic Protected Health Information.
9. Provide an Audit function for Security Incidents that is used to establish patterns of intentional activity, or to identify deficiencies in existing Security Mechanisms.
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. The HIPAA Regulations under 45 CFR §164 require the following be implemented:
         a) Identification of a Security Incident Response Team or teams.
         b) Mechanisms to detect security incidents
         c) Formal response procedures
         d) Procedures to facilitate reporting of information Security Incidents and their outcomes.
         e) Investigate factors that contribute to the Security Incidents, and any violations of the ACE governance security policies, or the Security Rule.
         f) Respond to Business Associate reported Security Incidents.
         g) Distribute software Security Mechanisms, as considered reasonable and appropriate, to avert or contain Information Systems Security Threats and attacks to Electronic Protected Health Information.

      3. A Security Incident can consist of any one or more of the following conditions:
         a) A breach, an attempted breach or other Unauthorized Access of an ACE information technology asset. The incident may originate from the ACE network, or an outside entity.
         b) Internet worms or viruses.
         c) Conduct using an ACE information technology asset, which could be construed as harassing, or in violation of the ACE policies.
         d) Potential violation of Federal law, Virginia law or the ACE policy involving an ACE information technology asset.

   B. Responsibilities:
      1. The designated ACE Information Security Official is responsible for the overall Security Incident Reporting and Response Program.
      2. The Security Official will work with component organization Information Security Official(s) and Resource Owners to develop the details of how incidents will be dealt with. These specific processes will include:
         a) How members of the Workforce are to report Security Incidents. (Initially this reporting will be via a call to the Information Systems Service Desk.)
         b) Determine how reported incidents will be triaged and initially addressed including determination of when a Security Incident “Computer Emergency Response Team” should be engaged to address major incidents.
         c) Determine how incidents will be documented, stored, and analyzed, and what type of reporting will be done as follow-up to any successful intrusions or other incidents.
         d) Linkage to Workforce management and Human Resources personnel in situations where follow-up disciplinary action and sanctions are required.
         e) Summary reports of the resources that are auto-monitored.
      3. The ACE Information Security Official will notify the Computer Emergency Response Team of any suspected or confirmed Security Incident involving an information technology asset of the ACE deemed serious enough to require immediate attention.
      4. Workforce members should follow the steps below when reporting Security Incidents:
a) Identify if the incident involves a compromised computer system or device. If so, the following steps should be implemented, immediately:
   i) Do not alter the state of the computer system. These computer systems should remain on and all of the currently running computer programs left as is.
   ii) Do not shutdown the computer, restart the computer, or disconnect the electrical connection to the computer.
   iii) Disconnect the computer from the network, by removing the patch cable from the back of the computer or disabling the network port.
   Immediately report the Security Incident to the Information Systems Service Desk and, if appropriate, to the assigned Resource Owner. The ACE Computer Emergency Response Team is charged with determining the appropriate response.

5. The ACE Information Security Official in cooperation with Purchasing will establish a program for reporting incidents relating to the component organization’s Business Associates and will establish a process for periodic review of the security of the Business Associate’s operations.

6. The ACE Information Security Official, in conjunction with the Resource Owners and the Information Systems groups, will work to continuously evaluate the automation of reporting Security Attacks and alerts, and the ongoing tightening of the Security of the ACE’s 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)(6)(i).
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.