SUBJECT: POLICY NO.: ACE-0009
APPROVED DATE 10/19/2005

Contingency Plan
EFFECTIVE DATE: 11/19/2005
SR-308a7i REVIEWED DATE:
SUPERSEDES NO.: NEW

I. PURPOSE:
The Contingency Plan represents the collaborative efforts of all component organizations of the Affiliated Covered Entity (ACE) to respond quickly and effectively to an Emergency or other occurrence that could damage or destroy Information Systems that receive, create, maintain, or transmit Electronic Protected Health Information.

II. POLICY:
A. The ACE shall prepare in advance for response to the loss of Access to computer systems and information due to planned or unplanned events. The Contingency Plans will cover operations during the period when Access is not available, recovery of information generated, actions that occurred during the outage, and means to recover damaged computer systems to their state at the time of the incident.

B. The ACE will tie the Information Security Contingency Plans tightly with the overall operational plans for dealing with various types of Emergency situations.

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. All computing resources shall be assigned a Resource Owner who is responsible for the Integrity, Confidentiality, and Security of the resource.
3. The existing Emergency Planning Policies and Procedures consider the operational impact of Information Systems unavailability and the handling of these during Emergencies and during follow-up activities.
4. Several of the ACE component organizations have policies that provide the basis for describing communications, responsibilities, and actions taken during and after a computer systems outage.

B. Responsibilities:
1. The owners of computing resources containing Electronic Protected Health Information are responsible for assuring that those resources are appropriately backed-up and protected, and that the state of the resource can be recovered to a point close to the point of any service interruption.
2. The Resource Owners, along with the Compliance Office, the Information Systems departments, and the Information Security Officials, have an ongoing responsibility to effectively secure and protect vital information from Threat, harm, or loss.
3. The Managers of the Workforce are responsible for informing personnel on the policies and procedures to be utilized during an outage situation and to recover the systems to currency once the Emergency / outage is over. The steps required for such operations should be documented in
unit-specific procedures and processes, as necessary to assure that
these procedures are understood and followed.

4. The Information Security Officials, along with the Information Systems
Directors and the operational management involved in Emergency
situations, have responsibility for conducting reviews of each such
event and for determining areas for improvement.

5. The designated ACE Information Security Official is responsible for the
ongoing review of potential increased Threats to the Security of the
protected data that could be present during Emergencies.

6. The Compliance Office and the Information Security Officials are
responsible for assessing the ability of Resource Owners to recover
resources (Data Backup Plans / Disaster Recovery Plans) if necessary
during a scheduled periodic review of the computing resources.

7. The designated Information Security Official, along with the IT Steering
Committee, will review the categorization of the various Information
Systems used by the ACE and the status of the Back-Up, Recovery,
Emergency Mode Operations and Testing plans associated with each,
whenever a major change is made or when otherwise appropriate.

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)(7)(i).
B. VCU Health Systems — Glossary of HIPAA Terms
C. VCU Health Systems Compliance Manual
D. Implementation Directive – ACE-0002

APPROVED:

Signature on File

Dr. Sheldon M. Retchin, M.D., M.S.P.H.