ADAMHS BOARD FOR MONTGOMERY COUNTY	**BP #** 527	
TITLE: Security Incident Response and Reporting	**SUBJECT** HIPAA SECURITY	
Page 1 of 3	**EFFECTIVE DATE** 8/2/06	**SUPERSEDES DATE** 4/27/05

PURPOSE: To guide the Board reporting of and response to incidents that threaten the privacy, integrity, or availability of information stored on its information systems. Security Incidents include, but are not limited to:

- Attempted or actual violations of Board information system security policies, particularly those that compromise or threaten to compromise electronic protected health information or other non-public information maintained by the Board.
- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Infection by virus or other malicious software
- Failure of system hardware, firmware, or software

POLICY:

1. Any officer, employee or agent of the Alcohol, Drug Addiction and Mental Health Services Board for Montgomery County who believes another officer, employee or agent of the Alcohol, Drug Addiction and Mental Health Services Board for Montgomery County has breached the facility's privacy or security policies and/or procedures or otherwise breached the integrity or confidentiality of member/client or other sensitive information shall immediately report such breach to his or her superior or to the Privacy or Security Officer. Workforce members shall report suspected electronic security incidents upon detection to the HIPAA Security Officer.
2. The Network Administrator shall be responsible for assessing reports of unusual security events, evaluating their degree of threat, and initiating and coordinating the appropriate level of response. These incidents will be reported to the HIPAA Security Officer.
3. The incident response process will provide an escalation mechanism, specifically:

Priority One - Protect individually identifiable health information and non-public information maintained on its systems. Prevent exploitation of networks, workstations, systems, or sites storing individually identifiable health information or other confidential information. Inform affected users about penetrations that have already occurred.

Priority Two- Protect other data, including managerial. Prevent exploitation of other systems, networks or sites and inform already affected systems, networks or sites about successful penetrations.

Priority Three - Prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.).

Priority Four - Minimize disruption of computing resources (including processes). It is better in many cases, to shut a system down or disconnect from a network, than to risk damage to data or systems. The Network Administrator shall work with each data and system owner to evaluate the trade-off between shutting down and disconnecting, and staying active.

4. The Board shall establish and maintain reasonable and appropriate methods for monitoring activity on its information systems.

5. All modes of information about system use will be regularly monitored for signs of anomalous activity and any anomalous activity that appears to represent a breach of security or a disruption/degradation of system performance shall be thoroughly investigated to determine its origin, scope and methods.

6. All anomalous events requiring investigation shall be documented in accordance with the standard procedure for making Security Incident investigation reports.

7. Information Security Incidents will be handled in a manner that meets the following standards:

- Minimizes adverse consequences to the Board's resources, employees, and customers.
- Prevents or discourages repetition of incidents.
- Meets reporting requirements specified in Board security policies and procedures as well as applicable law.
- Assures that all violators are reported to the proper authorities.
- Provides feedback to assist the Security Officer, Network Administrator, and management in identifying and correcting inadequacies in Board security policies and procedures.
- Follows Board Policy 504, "Sanctions for Breach of Privacy and Security of PHI" and subsequent procedures.

8. All Security Incident reports shall be retained for 6 years.
9. An annual calendar year report shall be produced by Security Officer and distributed to the Executive Director and the Director of Business Operations.
10. Annually, the security incident report will be discussed with all staff to further reduce the likelihood of such events.

REFERENCES:
HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp, February 20, 2003. § 164.308(a)(6).

"Information Security: An Introductory Resource Guide for Implementing the HIPAA Security Rule", National Institute for Standards and Technology (NIST), http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf, May 2004.

"CMS Information Systems Security Policy, Standards and Guidelines Handbook", Centers for Medicare and Medicaid Services, http://www.cms.hhs.gov/it/security/docs/handbook.pdf, July 2004.

C:\ADAMHSWEB\Policies\500-HIPAA\527_Mont_SecurityIncidentResponseandReporting.doc~~N:\Word Files\DOCS\ADAMHS Board Policies\Board Policies Current\500's – HIPAA\527_Mont_SecurityIncidentResponseandReporting.doc~~~~M:\AISProcedureManual\HIPAASECURITY\Mont_HIPAA SECURITY POLICIES\527_Mont_SecurityIncidentResponseandReporting_REV.doc~~