

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 529	
TITLE: Workstation Use & Security	SUBJECT HIPAA SECURITY	
Page 1 of 3	EFFECTIVE DATE 4/21/05	SUPERSEDES DATE

PURPOSE: To establish guidelines for workforce members that will ensure the proper use of workstations.

POLICY:

1. General Guidelines

- 1.1. Workstations are the property of the Board and are intended for official Board business purposes.
- 1.2. Limited personal use is permissible however it must be appropriate and subordinate to business use.
- 1.3. All users have the responsibility to use workstations, information system resources and services in an efficient, effective, ethical and lawful manner and to be aware of the ways their own use might have adverse impact on other users.
- 1.4. Workforce members are expected to know and understand Board security policies and exercise diligence in following them in order to properly protect the vast amount of individually identifiable health information that resides on its system.

2. Prohibited Uses of the Workstation

- 2.1. Unauthorized acquisition, disclosure, modification or destruction of any computerized information or attempting to do so.
- 2.2. Unauthorized modification of computer resources, including the computer, computer software and information. Modification includes any unauthorized changes, appending, replacement, and contamination of the resources or any act that would make the resource inaccurate, unsuitable or unavailable for its intended use.
- 2.3. Any unauthorized attempt to obtain a Board log-in ID or password that belongs to another user.
- 2.4. Any use of the Board owned computer resources in the commission or attempted commission of a misdemeanor or felony crime or aiding, abetting, soliciting or conspiring to commit a crime.
- 2.5. Unauthorized use or access and/or attempted unauthorized use or access to Board information systems including but not limited to, all computers and information stored therein.

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 529	
TITLE: Workstation Use & Security	SUBJECT HIPAA SECURITY	
Page 2 of 3	EFFECTIVE DATE 4/21/05	SUPERSEDES DATE

2.6. Unauthorized acquisition, disclosure, modification or destruction of any computerized information that supports Board business or the attempt to do so.

2.7. Installation of any software on Board equipment that has not been specifically approved by Manager of Information Systems or the Network Administrator.

2.8. Logging onto any system with any identification or password other than that assigned to the user.

2.9. No user shall attempt to disable, defeat or circumvent any Board supported security feature or assist anyone else in doing so.

2.10. No user shall setup, install, or operate any type of peer to peer based file sharing program on the Board's network.

3. User Privacy Expectations and Board Rights

3.1. System users are granted access to computer and information resources to assist them in performance of their jobs. Users do not have an absolute right to privacy in anything they create, and store on Board systems.

3.2. The Board retains the right to monitor usage of any and all aspects of its telecommunications and computer systems including user voice-mail, networks, intranet and internet to ensure compliance with its policies and with relevant laws. This includes the right to perform manual or automated audits of system use and contents.

4. Privacy

4.1. Electronic records generated on Board systems, may be public records. There is no reasonable expectation of privacy with regard to the use of the Board network.

4.2. Workforce members will follow all Board security and privacy policies with regards to individually identifiable health information that resides on the workstations and the associated networks. All workforce members are expected to know and understand Board privacy and security policies and procedures.

5. Security

5.1. Users are expected to be vigilant in maintaining system security and shall notify the Manager of information systems or the Network Administrator of any security weakness or breach.

5.2. Users shall follow all account authorization and log-on/log-off procedures.

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 529	
TITLE: Workstation Use & Security	SUBJECT HIPAA SECURITY	
Page 3 of 3	EFFECTIVE DATE 4/21/05	SUPERSEDES DATE

5.3. Users shall maintain local passwords in accordance with the Board's policy on passwords and follow password protection guidelines.

5.4. All workforce members are expected to know and understand Board security policies and procedures.

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. § 164.310(b) & (c).

"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.