

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 516	
TITLE: Access Controls	SUBJECT HIPAA SECURITY	
Page 1 of 2	EFFECTIVE DATE 08/02/06	SUPERSEDES DATE 4/27/05

PURPOSE: To guard electronic protected health information (EPHI) from unauthorized access and ensure appropriate levels of access to EPHI based upon each staff person's organizational role.

POLICY: 1. Unique Account Identification

Each information system user shall have exclusive access to one account (User ID) assigned to them. Special function specific accounts will be utilized in the system for security reasons, such as a "backup" account.

2. Emergency Access

EPHI shall be protected and made available to authorized users in the event of an emergency. All domain administrators will deposit current passwords in secure area for emergency retrieval purposes.

3. Automatic Lockout

All user sessions will automatically lock out to the screen saver after 10 minutes of inactivity.

4. Off Site (Out of the office) Access

- a. All access that is allowed below should be performed when there is no other browser or email package open.
- b. Off Site access by staff to email is acceptable.
- c. Off Site access by Staff to any internal network location is not acceptable with exceptions. Exceptions are FTP access to the 1) FTP server and the 2) Web Server. Upon a security emergency, the HIPAA Security Officer may approve temporary access in writing to specific staff with time span specified.
- d. Off Site access via secure internet FTP by BH Providers and other entities is acceptable upon approval by the HIPAA Security officer. This access is acceptable only from their offices.
- e. Off Site access to network locations via secure internet connection is acceptable when other entity is under contract for such access. This access is acceptable only from their office locations.

Formatted

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 516	
TITLE: Access Controls	SUBJECT HIPAA SECURITY	
Page 2 of 2	EFFECTIVE DATE 08/02/06	SUPERSEDES DATE 4/27/05

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. § 164.312(a)(1), (a)(2)(i), (a)(2)(ii), (a)(2)(iii), and (a)(2)(iv).

“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.