

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 522	
TITLE: Guarding Against, Detecting and Reporting Malicious Software	SUBJECT HIPAA SECURITY	
Page 1 of 2	EFFECTIVE DATE 4/21/05	SUPERSEDES DATE

PURPOSE: To guide the ADAMHS Board for Montgomery County in implementing measures to detect and report on the intrusion of malicious software. Malicious software (e.g. virus software or spyware) can be the source of system security breaches and can also compromise the integrity and validity of the data stored in such systems.

POLICY:

1. To ensure that information systems are protected against malicious software, the Network Administrator must implement safeguards to protect said systems. These safeguards will include:
 - 1.1. Implementation of a virus detection system, preferably of the enterprise variety, which allows for automatic signature updates and for logging and various modes of notification when infection attempts are detected.
 - 1.2. Operating system policies that prevent users from installing software.
 - 1.3. Firewall and or SPAM(Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail) control policies that prevent non-approved files from being procured by or pushed out to users.
 - 1.4. Anti-spyware/Adware software to assist in mitigating the affects of such rogue software.
2. The Network Administrator must keep abreast of current malicious software threats.
3. The Network Administrator is responsible for training and educating the workforce to become participants in the identification of and protection against malicious software.
4. The workforce employees are to report suspect activity to the Network Administrator.
5. The Network Administrator will implement procedures and mechanisms to track and report to the appropriate management and security personnel when malicious software infiltrations are identified.

REFERENCES:

ADAMHS BOARD FOR MONTGOMERY COUNTY	BP # 522	
TITLE: Guarding Against, Detecting and Reporting Malicious Software	SUBJECT HIPAA SECURITY	
Page 2 of 2	EFFECTIVE DATE 4/21/05	SUPERSEDES DATE

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)(5)(ii)(B).