Subject: Anti-virus Software Policy

Scope: Faculty, Staff, and Students that Utilize HIT Supported Devices and Network

Effective Date: 1/01/2005
Last Review/Revise Date: 12/10/2012
Responsible Department: Health Information Technology

Policy
All systems purchased and supported by Health Information Technology (HIT) with have antivirus software and virus definition files that HIT updates on at least a monthly basis.

Purpose
This policy is designed to help prevent infection of Health Information Technology supported computers and computer systems by computer viruses and other malicious code that could compromise security.

Definitions
Antivirus Software: “antivirus” is protective software designed to defend your computer against malicious software. Malicious software, or “malware” includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents. In order to be an effective defense, your antivirus software needs to run in the background at all times, and should be kept updated so it recognizes new versions of malicious software.

Virus Definition Files: Conventional virus scanners rely on virus definition files to perform their work. These files (there may be only a single file for some scanners) contain the patterns that they use to identify viruses. The definition files tell the scanner what to look for to spot viruses in infected files. Most scanners use separate files in this manner instead of encoding the virus patterns into the software, to enable easy updating.

Process
1. All computers attached to the msufgp/hc.msu.edu domain must be installed with the standard, supported anti-virus software that is available from HIT. After installation by HIT, anti-virus software updates will automatically install as they become available.

2. Users must never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then “double delete” them by emptying your Trash.