Malicious Software Prevention

Introduction
Malicious software can disrupt the normal operations of information systems or allow an unauthorized user to gain control of basic information systems functions, and data, including access to sensitive and confidential information. Malicious software can attack any kind of networked device. It can be transferred from workstation to workstation by many devices, including use of the Intranet, the Company network or mobile media like USB drives or CDs. This section outlines the responsibilities and safeguards that are required to minimize the risks.

Malware Prevention: User Responsibilities
Most malicious software tries to take advantage of the normal activities of workstation users, so security-aware users can limit the risk of infection by the following behaviors:

- Report problems that may be malicious software to IS/IT and let them run the appropriate checks and make repairs, if necessary. These may include, but are not limited to the following:
  - Warnings from anti-virus software.
  - Serious and abrupt changes in performance – slow downs.
  - Excessive pop-up screens, especially when using the web.
  - Changes in the appearance of your anti-virus icon.

- Limit browsing to reputable, well-known web sites, especially when you are not connected to the web at a Company location, i.e., traveling and using the VPN.

- Do not open an e-mail attachment, or click on a link in an e-mail from an unknown sender or from a known sender if it’s unexpected or suspicious, especially if the e-mail comes from a non-FMCNA address. Check with the sender first.

- Limit downloads of files and software from the web to only items that you need to do your job, from known, secure web sites.

- Read pop-up boxes and do not click on “OK” unless you understand the message and its risks. Otherwise, close them with the “x” at the top right corner or ask for help. Excessive pop-up boxes when you use the web are a potential symptom of some kinds of malicious software and should be reported as above.

- Do not accept pop-up boxes that offer upgrades to installed software. If you need a software upgrade, contact IS/IT to have it done.

Continued on next page
Malicious Software Prevention, Continued

- Do not install or use software applications and programs that are not approved by IS/IT or Network Security.

IS/IT responsibilities to minimize risks from malicious software are as follows:
- Select and support reasonably up to date versions of anti-virus software for all workstations, as appropriate to the risk of infection.
- Assure that anti-virus software and virus definitions are kept reasonably up to date.
- Monitor for infected workstations and clean infections from machines where the anti-virus software could not contain or clean it automatically.
- Investigate complaints from end users that may be related to malicious software infections and clean or re-image infected machines.
- Maintain a software upgrade program that applies security patches in a timeframe that’s appropriate to the risk that vulnerabilities will be exploited by malicious software.
- Analyze malicious software infections for risk to PI/PHI and be prepared to respond to an incident that may threaten it.