Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Protection from Malicious Software*

HIPAA Regulation:

- *Protection from malicious software* §164.308(a)(5) addressable

Policy Purpose:

The purpose of this policy is to establish criteria for protections to guard against, detect, and report malicious software. Malicious software includes, but is not limited to, viruses, worms, malware, and spyware.

Policy Description:

Saratoga Bridges shall ensure that all workstations install and maintain current anti-virus software. All workstations shall be configured to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.

In the event that a virus, worm, or other malicious code has infected or been identified on a server or workstation that poses a significant risk, that equipment shall be disconnected from the network until it has been appropriately cleaned.

Policy Responsibilities:

Workforce Member Responsibilities

1. Disabling automatic virus scanning features is prohibited.
2. Maintain current anti-virus software on their non-**Saratoga Bridges** computer that is used to access EPHI.
3. Immediately contact the manager or supervisor and the IT Service Desk if a virus is suspected, as explained in the ***Security Incident Reporting, Risk Assessment, and Response Policy***.

IT Support Responsibilities

1. Maintain current anti-virus software on all HIPAA covered component workstations.
2. Configure laptops to activate and update anti-virus software automatically whenever the computer is turned on and connected to the network.
3. Inform supervisors/department heads/management of any new virus, worm, or other malicious code that may be a threat to EPHI.
4. Disconnect any server or workstation from the network until it has been appropriately cleaned if infected by a virus, worm, or other malicious code that poses a threat to EPHI.

Manager and Supervisor Responsibilities

1. Ensure that laptops used to logon to the network shall have all anti-virus software updates installed by IT support.
2. Ensure that workforce members are made aware of the threats and vulnerabilities due to malicious code and software such as viruses and worms.
3. Inform workforce members of any new virus, worm, or other type of malicious code that may be a threat to EPHI.

Anti-Virus Process Guidelines

Recommended processes to prevent virus problems are as follows:

- Always run the corporate standard; supported anti-virus software is available from the IT Department.
- 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 bin.
- Delete spam, chain, and other junk email without forwarding, in accordance with **Saratoga Bridges *Acceptable Use Policy***.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.