HIPAA Security – Protection from Malicious Software AD.HS45

POLICY:

Lifesong Hospice and Palliative Care has systems and processes in place for preventing, detecting and reporting malicious software.

PROCEDURE:

1. Anti-virus software with current virus definition files is installed on all desktops, laptops and servers and programmed to conduct automatic virus scanning.

2. Security patches and updates for computer operating systems and software are regularly installed to reduce known vulnerabilities.

3. Hospice co-workers are not allowed to download or install software on desktops or laptops without prior authorization.

4. Hospice co-workers are not allowed to open email attachments from unknown or untrustworthy sources.

5. All email attachments from known and trustworthy sources must be scanned for the presence of viruses.

6. When the presence of a virus is suspected, or detected, the Security Officer or designee must be notified as soon as possible.

7. Hospice co-workers are not allowed to proceed with virus eradication efforts without authorization and supervision.

8. When a computer virus is suspected or detected, the infected machine and any others that may have been contaminated must be isolated from the network, be scanned, and repaired.

9. Hospice co-workers receive periodic security reminders regarding their responsibilities with respect to guarding against, detecting and reporting malicious software.

10. Protection from malicious software is included in the hospice's security training program.

11. Sanctions are applied against hospice co-workers who violate the hospice's protection from malicious software procedures and practices.

Created:	Reviewed:	Revised:	Effective:
05/2018	11/2018		4/2019