**POLICY & PROCEDURES**

***Defining the Overall Approach toward Meeting a Requirement***

### **Protection from Malicious Software §164.308(a)(5)(ii)(B)**

### **Effective Date:** <Month Day, Year>

### **Policy Number:** <If applicable> **Rev.** 0

**Policy:** We must develop, implement, and regularly review a documented process for guarding against, detecting and reporting malicious software that poses a risk to our information systems and data. All of our workforce members must be trained and reminded about this process. Unless appropriately authorized, our workforce members must not bypass or disable anti-virus software.

**Procedures:** We are responsible for obtaining appropriate software to detect malicious software, viruses, worms, and malicious codes that might affect our information systems containing ePHI. Workforce members are trained regarding this software's use. Our workforce members will not bypass or disable it without proper authorization from our Security Official.

**Details:** The protection from malicious software procedures include but are not limited to:

* Workforce members receive training on what to do if they suspect a computer virus or receive a suspicious email message.
* Information systems are protected using operating system security updates and appropriate antivirus software to effectively detect and prevent malicious software, particularly viruses, worms and malicious code.
* Malicious software prevention, detection and reporting processes may include:
* Installation of operating system security patches and updates.
* Installation and regular updating of antivirus software on all information systems.
* Periodic scans of workstations for the presence of malicious software.
* Automatic scans of electronic mail attachments for malicious software.
* Workforce members reporting suspected or known malicious software.
* Systems found to be infected will be not be used and if possible removed from the network until the infection is removed or the system is reformatted.
* Protection from malicious software training will cover topics such as:
* Identifying malicious software and phishing email messages.
* Reporting suspicious or malicious software.
* How to avoid downloading or receiving malicious software.
* Why web browser security settings should not be changed.
* Documentation (e.g. training materials, vendor antivirus software contracts) of the practices in place will be retained as evidence of compliance.

**Location of supporting documentation:** If so, identify the document and location it is stored here.

## REVISION HISTORY

| Revision | Date | Initiator | Nature of Change |
| --- | --- | --- | --- |
| 0 |  |  | Initial draft |
| 1 |  |  |  |