Protection from Malicious Software Policy

BACKGROUND:

The Health Insurance Portability and Accountability Act of 1996 *(HIPAA)* requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI *(ePHI)* data. According to the law, all workforce members within [Insert Covered Entity or Business Associate name] must preserve the integrity and the confidentiality of individually identifiable health information *(IIHI)* pertaining to each patient or client.

PURPOSE:

Each department, which handles ePHI, will effectively communicate security processes used to protect the confidentiality, availability and integrity of ePHI.

DEFINITIONS:

1. Electronic Protected Health Information (ePHI): Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. ePHI does not include students records held by educational institutions or employment records held by employers.
2. Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including demographic information collected from an individual, and:
   1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse.
   2. Relates to the past, present, or future physical or mental health or condition of an individual, or the past, present, or future payment for the provision of health care to an individual.
   3. That identifies the individual.
   4. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
3. Security Officer: the individual appointed by [Insert Covered Entity or Business Associate name] to be the HIPAA Security Officer under §164.306(2) of the HIPAA Security Rule.
4. Malicious software (malware): Any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc.

PROCEDURES:

1. [Insert Covered Entity or Business Associate name] will develop, implement, and periodically review a documented process for guarding against, detecting and reporting malicious software posing a risk to ePHI. Malicious software prevention, detection, and reporting procedures will include, but are not limited to:
   1. Anti-malicious software installed and updated on ePHI Systems.
   2. Procedures for [Insert Covered Entity or Business Associate name] workforce members to report suspected or confirmed malicious software.
   3. Plan for recovering from malicious software attacks in accordance with the Disaster Recovery Plan.
   4. Process to examine electronic mail attachments and downloads before they can be used on ePHI Systems.
2. [Insert Covered Entity or Business Associate name] workforce members will not bypass or disable anti-malicious software installed on ePHI Systems unless properly authorized to do so.
3. [Insert Covered Entity or Business Associate name] will provide periodic training and awareness to its workforce members about guarding against, detecting, and reporting malicious software. Training and awareness for workforce members on protection from malicious software will include, for example, the following topics:
   1. How to discover malicious software
   2. How to report malicious software
   3. How to discover malicious software fraud
   4. How to keep from downloading or receiving malicious software including not opening or launching email attachments that may contain malicious software
   5. How to use anti-malicious software appropriately

**VIOLATIONS:**

Any known violations of this policy should be reported to the Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with [Insert Covered Entity or Business Associate name] procedures. The [Insert Covered Entity or Business Associate name] may advise law enforcement agencies when a criminal offense may have been committed.