POLICY & PROCEDURE

(EXAMPLE FOR INFORMATIONAL PURPOSES ONLY)

Title: Security Awareness Training & Reminders	
No: XXX.XXX **Version:** V3.0	**Approved By:** Name(s) **Signature:** _____ **Approval Date:** XX/XX/XXXX **Effective Date:** XX/XX/XXXX **Last Reviewed Date:** XX/XX/XXXX
Authorities & References: HIPAA - §164.308(a)(5)(i), §164.308(a)(5)(ii)(A)	

Purpose

To provide appropriate security awareness training and reminders to workforce to reduce the risks of security violations or breaches.

Policy

All [Organization] workforce members shall receive appropriate training concerning [Organization]'s security policies and procedures. Such training shall be provided to all new employees and shall be repeated at a minimum annually or when any major changes to the organization occurs for all employees. Security training must be complete before new hires are provided access or accounts to the information systems.

[Organization]'s Information Security Officer, or designee, shall provide periodic security reminders by email to applicable workforce members.

Security training will include procedures in place regarding password management, monitoring log-in attempts, and anti-virus for guarding against, detecting, and reporting malicious software.

Procedures

1. Security Training Program
   The Security Officer shall have responsibility for the development and delivery of initial security training
   a. All workforce members shall receive such initial training addressing the requirements of the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation for all training activities.
   b. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.
   c. The Security training shall include, but is not limited to, the following topics:
      i. If applicable our information security policies, procedures, and standards;
      ii. secure use of our information systems (e.g., log-on monitoring, allowed software, restricted downloading);
      iii. significant risks to the information systems and data;
      iv. legal and business responsibilities for protecting its information systems and data;
      v. Protection from malicious software, including, but not limited to:

1. The malicious software protection mechanism that has been implemented;
2. Information system protection capabilities;
3. Workforce members roles and responsibilities in malicious software protection procedures;
4. Steps to protect against malicious software;
5. Steps to detect malicious software;
6. Action(s) to be taken in response to malicious software detection.

vi. Password management;
vii. Contingency plans for emergencies and disasters that damage the confidentiality, integrity, or availability of its information systems;
viii. Procedures for reporting a privacy or security violation;
ix. Monitoring of log-in attempts, how to identify inappropriate or attempted log-in attempts, actions to be taken in response to an inappropriate log-in attempt;
x. Reporting discrepancies.

2. Security Reminders
   The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis.
   a. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, and discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.
   b. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

3. Protection from Malicious Software
   As part of the Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
   a. Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail;
   b. The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current;
   c. Instructions to never download files from unknown or suspicious sources;
   d. Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software;
   e. The importance of backing up critical data on a regular basis and storing the data in a safe place;
   f. Damage caused by viruses and worms; and what to do if a virus or worm is detected.

Document Control

Reviewed / Revision No	Date	Authorized Personnel	Summary of Change(s)