Policy 4
Security Awareness and Training Policy and Procedure

Policy:

1. Security Reminders

The Security Officer will be responsible for communicating security reminders to employees. The Security Officer has discretion to determine the exact method of communication and may take into account feedback from employees regarding their preferred method of learning and their learning needs. Examples of ways in which security reminders may be communicated, include, but are not limited to:

- Security Reminder posters
- Security newsletters
- Security reminders during staff meetings
- E-mail reminders

The topics to be addressed in these communications will be determined by the Security Officer. The issues that the Security Officer may consider when determining appropriate content for reminders should include, without limitation, the following:

- Security issues brought to the attention of the Security Officer (such as breaches of the policies)
- Questions raised by staff
- New guidance from the government regarding steps necessary for compliance with the HIPAA Security Rule
- New policies and procedures implemented by the practice

2. Protection from Malicious Software

In order to protect the practice from the introduction of malicious software into the practice's information systems, employees are responsible for complying with the following guidelines:

- Employees are not permitted to add or download software programs to workstations without first consulting with the Security Officer or a person authorized by the Security Officer to give such approval.
- Employees are not permitted to open attachments associated with personal e-mail (for example, jokes, video clips) since these types of attachments are often used as a mechanism to spread viruses and other malicious software.
- Employees are not permitted to open e-mail attachments from individuals who they do not know.
- Employees are expected to alert the Security Officer or person designated by the Security Officer if they receive a suspicious e-mail.

- Employees who receive e-mails warning of new virus threats should forward such e-mails to the Security Officer to determine whether the threat is realistic or a hoax.
- Employees are not permitted to disable anti-virus software installed on their workstation.
- If anti-virus software detection does not run automatically, employees are responsible for running virus scans.

3. Log-in Monitoring

If employees are unable to log-in to a system for any reason, they should immediately contact the Security Officer or an individual designated by the Security Officer.

4. Password Management

When an employee requires access to an information system containing electronic protected health information, he or she will be provided with a password.

If employees are permitted to develop their own passwords, they should not use personal information that others would know, such as their own name, a spouse's name, a child's or pet's name.

If the system does not force employees to change passwords at least every six months, employees will be responsible for changing their own password every six months. If the employee does not know how to change the password, he/she is responsible for seeking guidance from the Security Officer or an individual designated by the Security Officer.

Employees are responsible for safeguarding passwords, including all of the following:

- Passwords should be remembered and should not be posted on computers, written on the back of name badges, kept in desk drawers, or kept in any other place where the password could be located by others.

- If an employee is having difficulty remembering his/her password, he/she should contact the Security Officer to assist with solutions, such as changing the password to something the employee can remember (but otherwise meets the guidelines set forth above).

- Passwords should not be shared with other employees under any circumstances.

- If an employee has reason to believe that another individual knows his or her password, the employee is responsible for changing the password or contacting the Security Officer.

Procedure:

1. The Security Officer will be responsible for establishing and adhering to a schedule for security reminders.
2. All employees will be responsible for reviewing the guidelines set forth in paragraph 2 above and any new policies that are developed with respect to malicious software.
3. All employees will be responsible for alerting the Security Officer of any log-in failures in accordance with Paragraph 3 above.
4. All employees are responsible for complying with the password management policies set forth above in Paragraph 4 and with any new policies that may be developed in the future related to password management.

Explanation of the Security Awareness and Training Standard and Explanation of the Security Awareness and Training Policy and Procedure

The "Security Awareness and Training" standard requires all covered entities to train all employees on HIPAA Security including ongoing updates and reinforcement. The four implementation specifications are (1) Security Reminders; (2) Protection from Malicious Software; (3) Log-in Monitoring; and (4) Password Management. Policy 4 is a sample "Security Awareness and Training" Policy addressing these specifications.

a. Security Reminders

The HIPAA Security Regulations require training that is an ongoing and evolving process. This includes initial training as well as "reminders". Some practical ways that reminders can be communicated may include posters, newsletters, staff meeting discussions, in-services or email reminders.

b. Protection from malicious software

Covered entities are also required to implement procedures to detect, report, and guard against malicious software. Malicious software is software that is designed to damage or disrupt a system. The most common example of malicious software is a "virus". Other examples of malicious software are "worms" and "Trojan horses."

Malicious software can be introduced into your systems in a number of ways. For example, a virus or worm might be attached to an e-mail or downloaded by a user from the internet. Malicious software is often sent or presented in a manner that tricks users into thinking it is an innocent application. For example, an e-mail may be sent with an intriguing subject line and an attachment that will activate malicious software as soon as it is opened. Another example would be a screensaver or computer game that can be downloaded from the internet, but actually has malicious software attached to it.

It is important that employees be trained on policies and procedures to prevent the introduction of malicious software. For example, employee training should include discussions regarding the need to refrain from downloading programs or files from the internet without prior authorization and policies against opening e-mails from sources that are unfamiliar or suspicious.

c. Log-in Monitoring

Log in monitoring involves the development and implementation of policies and procedures related to monitoring login attempts and reporting discrepancies.

For example, if a user gets an error message while trying to login, there is a risk that the user's password is being used by an unauthorized person. Users would be instructed on when and how to report such discrepancies.

d. Password management

Password management includes procedures and training regarding the creation of passwords, how to change passwords, and how to safeguard passwords.

If users are permitted to create their own passwords, certain guidelines should be in place. For example, most users would like to create a password that is easy to remember, such as their name or their spouse's name. However, such a password is also easy for others to guess. A combination of numbers and letters is more difficult to guess, as are passwords of a certain length, such as a minimum of seven letters. The organization must try to achieve a balance between making the password difficult to guess and keeping the password easy enough to remember so that the employee will not try to keep it posted at their workstation.

The organization should also determine the frequency with which passwords must be changed. Some systems have the capability to "force" users to change their passwords at set intervals. If systems do not have this capability, this should be addressed in written policies.

Employees should also be trained on how to appropriately safeguard their password. For example, passwords should not be written on workstations, kept in drawers or written on the back of name badges.