HIPAA Security Policy #5

Administrative Safeguards
Security Awareness and Training

Statement of Policy

The Company is a *Business Associate* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect The Company's commitment to complying with such Regulations. The Company will comply with the *Covered Entity's* documented HIPAA policies and procedures unless specifically stated in the below policy.

Purpose of Policy

The purpose of the policy is to develop a security awareness program that will train The Company's workforce members on how to reasonably protect and safeguard ePHI while allowing them to perform their job functions

Policy

5 Security Awareness and Training

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(5)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement a security awareness and training program for all members of its workforce including management."

1. All Company workforce must receive security training on how to protect the confidentiality, integrity, and availability of ePHI. Workforce members will not be allowed to access ePHI until they are properly trained on how to protect and safeguard the ePHI. The security and awareness program will include the following:

   i. Security reminders

   ii. Procedures for guarding against, detecting and reporting malicious software

   iii. Procedures for monitoring log-in attempts and reporting

   iv. Procedures for creating, changing and safeguarding passwords

2. The Company's HIPAA Security Officer will advise each existing workforce member (and new workforce members) of the level of training required and the procedure for completing training. The HIPAA Security Officer will keep a log containing the name of the workforce member, job classification, training level required, date the training was completed and date the training log was last reviewed for that employee. The Security Officer will continually track workforce members' training in the log to ensure that training

is completed in a timely manner and to reevaluate training needs when a workforce member's job function changes.

5.1 Security Reminders

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Periodic security updates."

1. The Company must develop and implement procedures to ensure that periodic security updates are issued to the workforce on reminders of or changes to The Company' HIPAA Security Policies.

2. The Company must develop and implement procedures to ensure that warnings are issued to the workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents. (See HIPAA Security Policy #6 -- Incident Response and Reporting).

Procedure

1. The Company will periodically provide Security updates and reminders to its workforce on how to protect and safeguard ePHI.

2. Security updates and reminders may be in the form of emails, videos, face to face presentations, posters or other methods to distribute the updates and reminders.

3. The Company will provide Security updates when any of the following occur;

    i. Significant changes to The Company' HIPAA Security Policies and Procedures.

    ii. Significant changes to safeguards or controls to protect ePHI.

    iii. Substantial risks to systems that contain ePHI.

5.2 Protection from Malicious Software

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Procedures for guarding against, detecting, and reporting malicious software."

1. The Company must develop and implement or follow a covered entity's procedures for guarding against, detecting and reporting to the appropriate persons, new and potential threats from malicious software such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

Procedure

1. The Company will ensure that all systems will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions.
2. The Company shall train its workforce members to identify and protect against malicious software. Periodic Security updates will be provided to all workforce members on how to identify and avoid malicious software.

3. The Company shall notify its workforce members of new and potential threats from malicious software designed to interfere with the normal operation of a system or its contents and procedures.

4. The Company's workforce members shall not try to bypass or disable the anti-virus / anti-malware software.

5.3 Log-in Monitoring

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Procedures for monitoring log-in attempts and reporting discrepancies."

1. The Company shall train its workforce members on monitoring Log-in attempts and reporting discrepancies that the workforce member becomes aware of.

Procedure

1. The Company's workforce members should expect that all activity on systems that contain ePHI will be logged and recorded. In addition, all changes made to ePHI will be logged and recorded.

2. The Company's workforce members should be trained on how to identify and report suspicious access activity on their workstations.

3. The Company' workforce members should be trained on any limitations on the number of failed login attempts that are permitted. In addition, workforce members should be trained that failed Log-in attempts will be logged and recorded.

5.4 Password Management

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(5)(ii)(D)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Procedures for creating, changing, and safeguarding passwords."

1. The Company must train its workforce members on creating, changing and safeguarding passwords in accordance with HIPAA Security Policy #14 - Access Control.

Procedure

1. The Company’s workforce members should receive training on the password policy that is defined in HIPAA Security Policy #14 - Access Control.

2. The Company’s workforce members should receive training on how to protect and safeguard passwords.