HIPAA Security Policy #3

Administrative Safeguards
Workforce Security Policy

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 ensure that all workforce members who need access to electronic Protected Health Information (ePHI) have the appropriate access while preventing all others from obtaining access to ePHI.

Policy

3 Workforce Security Policy

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(1)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) [Information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information."

1. The Company will ensure that only properly authorized workforce members shall have access to ePHI Systems. Workforce members shall not attempt to gain access to any ePHI that they are not properly authorized to access. The Company shall train its workforce members on proper and appropriate use of access rights.

2. The Company shall take reasonable and appropriate steps to ensure that workforce members who work with or have the ability to access ePHI are properly authorized and/or supervised.

3. The Company workforce members shall be screened, as appropriate, during the hiring process.

4. The Company shall implement a documented process for terminating access to ePHI when employment of workforce members ends or when access is no longer appropriate.

3.1 Authorization and Supervision

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(A)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed."

1. The Company will take reasonable and appropriate steps to ensure that workforce members who have the ability to access ePHI or work in areas where ePHI might be accessed shall be properly authorized and/or supervised. The Company will use a Minimum Necessary Policy, which is one of its HIPAA Privacy policies, and other policies as appropriate, as the basis for the type and extent of authorized access to ePHI.

Procedure

1. The Company will implement or follow a covered entity's procedures to ensure that only workforce members with a need to access ePHI are granted access to ePHI. No unauthorized access to ePHI will be allowed.

2. The Company shall maintain documentation detailing each workforce member's role and responsibilities, why such workforce member requires access to ePHI and the specific levels of ePHI access required by such workforce member.

3. The Company shall ensure that all workforce members who work with ePHI are supervised so that unauthorized access to ePHI is avoided. (See HIPAA Security Policy #4 – Information Access Management).

3.2 Workforce Clearance Procedure

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures to determine that the access of a workforce member to Electronic Protected Health Information (EPHI) is appropriate."

1. The Company shall develop and implement or follow a covered entity's procedures to ensure that the ePHI access of its workforce members is appropriate when granted and continues to be appropriate on an on-going basis. The Company shall maintain documentation detailing each workforce member's current role and responsibilities and the ePHI access required for such role and responsibilities. (See HIPAA Security Policy #4 -- Information Access Management).

Procedure

1. Each system manager (person who is responsible for the access levels and permissions of a system) shall perform an initial review for each system that uses ePHI to ensure that the current user list as well as the level of access for each user is appropriate. Each system manager should perform a subsequent review at least annually.

2. Each supervisor shall advise the appropriate system manager when a workforce member's role changes so that the workforce member's access level can be adjusted promptly.

3. The Company shall review prospective workforce members' backgrounds during the hiring process and, as appropriate, shall perform verification checks on prospective workforce members. The Company shall analyze prospective workforce members'

access to and expected abilities to modify or change ePHI as one of the bases for the type and number of verification checks conducted. Verification checks may include:

i. Confirmation of claimed academic and professional qualification

ii. Professional license validation

iii. Credit check

iv. Criminal background check

v. Other state or federal database checks

3.3 Termination Procedure

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(3)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section."

1. The Company shall develop and implement or follow a covered entity's procedures for terminating access to ePHI when the workforce member's employment ends or when the access granted is determined to be no longer appropriate. (See HIPAA Security Policy #4 – Information Access Management).

Procedure

1. The termination procedures should include the following steps:

    i. A notification mechanism to ensure that the appropriate personnel are made aware that the workforce member's access to ePHI is no longer required.

    ii. Recovery of all forms of access to PHI and ePHI that was granted or assigned to that workforce member. Examples include, but are not limited to, keys, remote access tokens, and identification badges.

    iii. Disabling the workforce member's accounts on networks and system.

    iv. Disabling remote access to networks and systems

    v. Changing administrative or other shared passwords of which the workforce member has been made aware.