HIPAA Security Policy #4

Administrative Safeguards
Information Access Management

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 describe the procedures that The Company should establish and implement to ensure that access to ePHI is assigned and managed in a manner commensurate with the role of each workforce member.

Policy

4. Information Access Management Policy

TYPE: Standard
REFERENCE: 45 CFR 164.308(a)(4)(i)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part."

1. This policy ensures that workforce members needing access to ePHI have appropriate access and provides procedural safeguards to ensure that access to ePHI is properly restricted. Before access to ePHI can be established for a workforce member, that workforce member must be authorized for the appropriate level of access that their position requires. Access to ePHI and systems that store or process ePHI requires a valid and authorized user account and password. Workforce members are required to authenticate themselves to these systems using their unique user accounts.

4.1 Access Authorization

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(4)(ii)(B)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

1. The Company shall implement or follow a covered entity's procedures to establish, document, periodically review and modify if appropriate each workforce member's right to access ePHI.

Procedure

1. Procedures for Access Authorization should include the following:

    i. Each supervisor or manager is responsible for authorizing access to systems and networks containing ePHI for his or her subordinates. Workforce members are not permitted to authorize their own access to ePHI or be granted authorization from another supervisor.

    ii. Each supervisor or manager is responsible for ensuring that the access to ePHI granted to each of his or her subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.

    iii. Each supervisor or manager is responsible for periodically reviewing the access to ePHI granted to each of his or her subordinates and for modifying such access if appropriate.

4.2 Access Establishment and Modification
IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 164.308(a)(4)(ii)(C)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement policies and procedures that, based upon the covered entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

1. The Company acknowledges that under The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") it is required to protect ePHI in the same regard as a covered entity.

2. The Company will create or follow a covered entity's documented process for establishing, documenting, reviewing, and modifying access to ePHI in accordance with The Company Information Access Management policy (Security Policy #4 – Information Access Management) and as set forth in the Access Authorization operational specification (see Security Policy #4.1 – Information Access Management). All requests for establishing or modifying access will be submitted in writing.

Procedure

1. Procedures for Access Establishment and Modification include:

    i. System managers shall implement a procedure for establishing and documenting different access levels to ePHI. System managers must define access levels for accessing ePHI. These access levels must be communicated to all supervisors of workforce members.

    ii. System managers shall implement a procedure for documenting establishment of access to ePHI. All requests for access or modification of access must be done in writing (or electronic) and copies of the request must be kept for at least 6 years

iii. System mangers shall implement a procedure for reviewing on a regular basis workforce members' access privilege to ePHI.

iv. System managers shall implement a procedure for modifying the access privileges of workforce members to ePHI, as appropriate, based on the periodic reviews.