AGENCY NAME		
Policy and Procedure		
Policy Number	Revision Number	Effective Date

Information Access Management

Background: ***164.308(a)(4)*** Information Access Management has to do with creation, administration, and oversight of policies to ensure that personnel is granted levels of access to electronic protected health information based on their responsibilities.

POLICY: It is the policy of _____*Community Services Board* to adhere to standards set by HIPAA and that only authorized personnel will be granted access electronic protected health information (PHI) by:

- Establishing an access privilege log
- Maintaining a record to track modifications to access rights and privileges

Isolating Health Care Clearinghouse Function

- Implementing procedures to isolate Health Care Clearinghouse functions to ensure that only authorized personnel have access to electronic PHI

Access Authorization

In order to appropriately comply with the Security Standards and effectively maintain healthcare operations, access will be determined by a role-based and context-based assessment:

- Access to a consumer's PHI will be available to the direct service provider, his/her immediate supervisor, and other providers on the same service unit/team
- Emergency Services/Crisis Intervention staff will have access to all consumers' PHI
- Direct service providers, Managers/Supervisors, Executive Director, Healthcare operations staff will have access to all consumers' PHI
- Medical Records staff will have access to consumers' PHI
- Reimbursement staff will have access to all consumers' PHI
- IT staff will have access to all consumers' PHI
- Data Entry staff will have access to all consumers' PHI, as needed, to complete

data entry

- Facility Coordinator and Facility Maintenance staff will not have access to any consumer PHI

Procedures to Ensure Appropriate Access and Access Authorization

- Upon hire, each staff member will be identified by the "class" in which their job functions fall
- *Human Resource staff or Supervisors* will ensure that new hires complete the appropriate *Access Request form* in order to establish the appropriate level of access, and request a unique user identification number; Supervisors must sign this form to verify accuracy
- IT staff will ensure that staff are trained during their orientation, to include information on the degree of access permissible by their job functions, security policies and procedures, and setting of passwords
- Removable media (i.e. diskettes, CD's, zip disks, etc.) that contain PHI will be secured at all times to prevent unauthorized access
    - If any removable media is lost or misplaced, an agency *Incident Form* must be completed by the staff member and processed as per the *Risk Management Policy*
- *All PHI is to be kept in the agency's client data system. In instances when PHI must be kept temporarily on individual hard drives, access must be limited by protecting the file.* .
- As per *County/City of*_____ IT policy, staff should log-off when leaving a workstation to prevent unauthorized access
- *Client Data System/ PC's* will have automatic lockout when the workstation has been unattended for ____ time, to ensure security of PHI and to prevent unauthorized access
- IT staff will periodically audit usage, to the degree possible, to identify any unauthorized access by staff
- IT staff will review, audit and modify access levels on a periodic basis
- Supervisors and IT staff will ensure that access to electronic PHI is terminated at an employee's termination from employment, and re-assessed for access limitations in the event of transfer from one job class (i.e. category) to another
    - *Supervisors* will ensure that all access devices are returned by the employee at the time of termination or transfer (if appropriate), and document this on the appropriate form
    - *Supervisors or Human Resources staff* will ensure that IT staff are informed of all staff terminations
    - In the event of an adverse staff termination, IT staff will be notified prior to informing the staff member, to ensure that information and

systems are protected from potential retaliation
- IT staff will remove the staff member's name from internal e-mail systems and system access lists, and disable access to the network

Physical Security -- The Human Resources Department will be responsible for providing keys and ID cards and assigning physical access privileges. *[In some organizations this is the responsibility of the IS department.]* Physical access privileges assigned to the workforce (usually employees and contractors) are used in conjunction with keys and ID cards. *[If ID cards are used, there may be corresponding badge readers.]* Physical access privileges are used to restrict entry into buildings and certain areas or rooms. Refer to the Policy for Physical Access Control. The Department is to keep a log of privilege assignments (refer to the Sample Access Privilege Log).

Access Establishment and Modification

Access controls have to do with restricting access to resources (e.g., paper, disks, workstations) and allowing only privileged entities (e.g., persons and applications) to access Protected Health Information. Individuals may, for example, have privileges based on the role of the individual, the time of day, the location, transaction type, department, or assigned by name. Examples of roles include a billing clerk or counselor working in Detox. The principal objective of access controls is to restrict access to only authorized entities.

Establishing access controls policy is the process for assigning privileges to people and other entities. It does not cover authentication of access control privileges via passwords or any other technical security services or mechanisms. Refer to the policies for Password Usage and Technical Security Services.

Establishing access controls is not to be confused with verifying identities. Refer to the policy and procedure for Verifying Identities.

Information System Access Security -- The Security Officer and Information Systems Department will be responsible for assigning Protected Health Information access privileges to authorized entities. The Department is to keep a log of privilege assignments (refer to the Sample Access Privilege Log).

A member of the workforce is not authorized to access another member of the workforce's client record or Designated Record Set unless it is for the purpose of treatment, payment or operations that is associated with the workforce member. The logs referred to above must be kept for six years. Refer to the Document Retention Policy.

AGENCY NAME		
Policy and Procedure		
Policy Number	Revision Number	Effective Date

The access control restrictions placed on the external users are the same or similar as the access control restrictions that are placed on internal users.

Relative to information system access, all authorized users will need to sign on to the network before signing on to specific applications or desktops.

Emergency access relating to treatment, payment, or health care operations must be provided. The Information System Department will provide the procedures for emergency access.

The Privacy and Security Officers will establish a written privileges matrix that relates roles or other categories to physical and information access privileges. An entity or person may have more than one role. *[This is where <<Informal Organization Name>> will want to add more specifics]*. The matrix will be used by the Human Resources and Information Systems Departments to assign privileges. The Privacy Officer must approve all exceptions to the privileges matrix in writing.

The Privacy and Security Officers will audit entities or persons with access to Protected Health Information once a year using, for example, sampling techniques or actual access logs for specific systems. The results of the audit are to be documented.