AGENCY NAME

Policy and Procedure

Policy Number	Revision Number	Effective Date

Workforce Security

Background: ***164.308(a)(3)*** The Security Rule under the Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to take reasonable steps to ensure workforce security that includes appropriate authorization and/or supervision of staff accessing electronic PHI, workforce clearance procedures, and termination procedures. This also means restricting access to Protected Health Information for only those entities that have access privileges.

Authorization and/or Supervision

The Security Officer will be responsible for the security infrastructure, training and oversight of computer and network maintenance personnel and will be accountable for:

- Developing and implementing security policies and procedures for _____________*Community Service Board*
- Training all members of the workforce on access methods to electronic systems and information
- Identifying the persons or classes of persons in the workforce who need access to PHI
- Identifying the category(ies) of PHI to which access is needed
- Implementing procedures:
    1. review appropriate use of access by staff ID to ensure that access to electronic PHI is limited to the persons or class of persons needing access to achieve the purpose of their job,
    2. for review and approval of requests for access and ensuring supervisory sign-off on security add/change/delete requests, and auditing outstanding access devices (e.g. keys, swipe cards, etc.) and are returned at the time of a staff termination
    3. monitor all access to high profile or VIP consumer records
    4. ensure required screen saver/terminal locking is executed

Workforce Clearance Procedure

An important part of the overall workforce clearance procedure is to ensure that individuals have the appropriate level of access and to prevent other workforce members who should not have access from gaining access. As __________________*(Client Data System)* develops the capability of electronically restricting access, implementation of access controls will be handled through the IS department.

Procedures:

- Upon hire, each staff member will be identified, cleared and recorded by the "class" in which their job functions fall before granting access to electronic protected health information
- The appropriate access level will be set according to the Information Access Management Policy.

Termination Procedures

- Supervisors, Security Officer 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 the Security Officer 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
- The Security Officer will ensure that the staff member's name from internal e-mail systems, system access lists, and disable access to the network