

PHYSICAL ACCESS CONTROLS POLICY

RESPONSIBILITY: Director of Information Systems, Security Official, and All Department Managers

BACKGROUND:

Physical access controls are rules for limiting access to safeguarded systems and data at all times and under all conditions. This includes maintaining access security during disaster recovery and emergency mode operations.

POLICY:

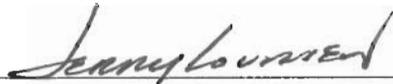
Behavioral Health and Health Facilities (BHHF) will maintain strict physical access controls to its information systems at all times and under all conditions. This includes the physical security of electronic and paper data. Physical access controls include the following:

- Disaster recovery: the same standard of physical access controls will be observed and maintained during disaster recovery procedures as apply during normal operations.
- Emergency mode operation: the same standard of physical access controls will be observed and maintained during emergency mode operations as apply during normal operations.
- Equipment and media control: safeguards to protect equipment and storage media from theft and damage when it is brought into or removed from BHHF facilities.
- A facility security plan and procedures for verifying access authorizations prior to granting physical access: protection from unauthorized entry or physical damage during and after business hours
- Maintenance records: records of repairs and modifications to hardware, software, locks, and facilities where protected health information is stored
- Sign-in procedure for visitors to sensitive areas, and escorts if appropriate
- Testing and revision of physical access control plans periodically.

These controls are to be detailed in a facilities security plan, which is maintained by the Security Official.

Effective Date: 4/14/03

Dates Revised:



Jerome E. Lovrien, Commissioner, Bureau for Behavioral Health and Health Facilities