Policy Number: HC-23	Page: 1	Of: 2
Title: Facility Security and Access Control		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) FACILITY SECURITY AND ACCESS CONTROL

All employees shall be aware of facility security and access policies to insure that only authorized personnel physical access to the facility and its equipment.

Audience

HIPAA Privacy / Security Officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.310(a)(1)

References

NIST SP 800-66

1) **Facility Security Planning**. The HIPAA Security Officer shall periodically evaluate physical security vulnerabilities, identify corrective measures, and develop a written facility security plan. The plan should focus especially on security of:
   a) Computer Servers
   b) Telephone and Networking equipment
   c) IT staff offices
   d) Workstation locations
   e) Individual Paper Records

   Attention should be given to areas with public access, whether workstations are protected from public access or viewing, the security of entrances and exits, and normal physical protections (locks on doors, windows, etc.).

2) **Employee Training**. The HIPAA Security Officer shall be responsible for employee training on their duties and responsibilities for facility security as described in the facility security plan.
3) **Maintenance of Physical Security Equipment**. The Operations Manager shall be responsible for maintaining equipment necessary to secure the facility, including locks,

alarm systems, doors, security lighting, etc. Records of repairs and modifications shall be maintained.

4) **Unauthorized Individuals**. Any staff who sees an unauthorized, unescorted person in the facility, except for those Public Access Areas, shall, in a polite manner, escort the person to a common area. Any suspicious incident shall be reported to the HIPAA Privacy/Security Officer and/or police.