Policy Number: HC-28	Page: 1	Of: 2
Title: Security Awareness Program		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) SECURITY AWARENESS PROGRAM

The board will conduct an ongoing security awareness program to train and refresh staff on the board's security policies. Priority topics shall include recognizing and avoiding malicious software, avoiding "social engineering" ploys, using passwords effectively, and adhering to workstation use policies.

Audience

Hipaa security officer

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.308(a)(5)

1) **Security Training Program for New Employees.** The HIPAA Security Officer shall develop, and maintain, a security training program for new employees. This should include, at a minimum:
   a) Password policies
   b) Recognizing and avoiding malicious software
   c) Understanding e-mail attachments
   d) Safe web browsing practices
   e) Dangers of downloading files from the internet
   f) Understanding of "Social Engineering" and how to recognize such ploys
   g) Knowledge of Workstation Use Policies
   h) Consequences for non-compliance
   i) Security Incident Reporting Procedures

   Other appropriate topics may be included at the discretion of the HIPAA Security Officer. The program may be conducted one-on-one, via e-learning system, or other media as determined by the HIPAA Security Officer.

2) **Upon initial implementation**, the Security Training program will be provided to all staff. Subsequently, all new staff should receive the training.
3) **Periodic security awareness training will offered to all employees**. The HIPAA Security Officer shall develop an annual plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; evaluation

and measurement techniques; and the frequency of training. Possible topics would include:

a) Reinforcement of topics for the Security Training Program and Security Policies
b) Advisories regarding current threats
c) Issues with new technologies such as smartphone/tablet security

A variety of media and avenues should be explored such as sign-in banners, security reminder cards for posting at workstations, articles in employee newsletters, posting on bulletin boards, etc. At a minimum, Computer Security Awareness will be included annually.