Policy Number: HC-37	Page: 1	Of: 2
Title: HIPAA Administrative Requirements Security Policies For All Staff-- **Security Incident Response and Reporting**		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) SECURITY INCIDENT RESPONSE AND REPORTING

The board will monitor all electronic information systems for breaches of security, mitigate harmful effects of security incidents to the extent practicable, and document any such security incidents and their outcomes.

Audience

All staff

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164; 164.308(a)(6)

(B) CREATION OF RESPONSE TEAM, CONTINGENCY PLANNING AND DRILLS

1) **Incident Response Team.** The HIPAA Security Officer is responsible for managing security incident response and reporting. As part of a pro-active management process, he or she may recommend to the Superintendent assignment of individuals for an Incident Response Team. The mandate to this group would be to coordinate the board's response to security incidents. This would include mitigation strategy, communications with law enforcement, the Individuals receiving services from the Board and the media.
2) **Contingency Plans.** The Incident Response Team may meet on a periodic basis to develop contingency plans, such as identification of a security consulting firm, public relations firm, or legal counsel who can be contacted in the event of a serious incident.
3) **Security Incident Drills.** The Incident Response Team may conduct security incident drills to develop skills and improve performance in the event of a serious security incident.

(C) SECURITY INCIDENT REPORTING AND RESPONSE PROCEDURE

1) **Reporting Security Incidents.** Any employee who becomes aware of a potential security incident must immediately contact the HIPAA Security Officer to report the incident.
2) **Response Procedure.** The HIPAA Security Officer and/or Incident Response Team will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident. Procedures specified in Breach Reporting and Duty to Report Violations and Security Incidents, Mitigation will be followed as appropriate.

The superintendent of the Board will be notified and any contingency plans will be activated.

3) **Documenting Security Incidents.** In conjunction with the HIPAA Security Officer, a written report must be filed within seventy-two hours (or as soon as practically possible) of becoming aware of the incident. The report should include
   a) Date and time of report
   b) Date and time of incident
   c) Description of circumstances
   d) Corrective action taken
   e) Mitigating action taken

   Documentation will be kept for 6 years.

4) **Post-Incident Analysis.** The HIPAA Security Officer and/or Incident Response Team will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response, and recommend to management any changes they believe appropriate.