Policy Number: HC-36	Page: 1	Of: 1
Title: HIPAA Administrative Requirements Security Policies For All Staff-- **Portable Computing Devices and Home Computer Use**		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A) Portable Computing Devices and Home Computer Use
Data on laptops should be encrypted and various security measures should be employed with employee-owned PDAs.

Audience

All staff

Authority

HIPAA Privacy and Security Rules, 45 CFR Part 164;
164.312(a)(2)(iv) Encryption and decryption

1) **Encryption on Laptops and other mobile devices.** Employees who use board provided laptop computers, smartphones, or other portable computing devices containing PHI shall use the encryption features to reduce the impact of disclosure in the event that the device is lost or stolen. The staff will use an encryption solution as detailed in Policy 3060 Technical Safeguards.
2) **Lost devices.** Employees must immediately report lost or stolen devices to their supervisor and the HIPAA Security Officer in accordance with the Security Incident procedure.
3) **Employee-owned portable computing devices.** Employees may not use their personal smartphones or other portable devices to conduct board activities.
4) **Work at home and use of employee's home computer.** Employees working at home and using their home computers for work purposes in general should avoid storing PHI on their home computers. Employees **must** consult with the HIPAA Security Officer regarding safeguards prior to storing any PHI on their home computers.
5) **Training.** The HIPAA Security Officer will provide training, as necessary, to employees on how to implement the security features required while using these devices.