Policy Number: HC-26	Page: 1	Of: 1
Title: Malicious Software Protection		
Regulatory Authority: HIPAA Regulations, FERPA Regulations, ORC, OAC		
Effective Date: 01/19/2021		
Reviewer/Job Title: Director of Operations		

(A)MALICIOUS SOFTWARE PROTECTION
All company computer systems will be protected by virus and malicious software protection capabilities.

Audience

Hipaa privacy/security officer

Authority

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

1) **Multi-Layered Defense Strategy.** The HIPAA Security Officer will insure that the computer network be protected from malicious software using a multi-layered defense strategy:
   a) Appropriately configured, commercial-grade firewall (per Policy 3060 Technical Safeguards)
   b) Centrally managed and updated anti-virus software
   c) DNS filtering service to limit connections to malicious sites, phishing attacks, and botnets per Policy 3060 Technical Safeguards
   d) Patching of operating system and application software per Policy 3060 Technical Safeguards
   e) Monitoring system logs per Policy 3020 Audit Control and Activity Log Review
2) **Special procedures** will be used, if appropriate, for any users who routinely access on-line banking accounts.
3) **Annual Review.** Annual review of this policy will be conducted to insure that the products, services, and configuration, and policies appropriately manage risk for this rapidly evolving threat.