MIS 28-Point HIPAA Checklist

Administrative

- ☑ Conduct and Document a Risk Analysis
- ☑ Develop and Maintain a Risk Mitigation Plan
- ☑ Establish a Sanction Policy
- ☑ Enforce Role-Based Access Controls
- ☑ Implement Secure Remote Access and BYOD Policies
- ☑ Require Acceptable Use Policy (AUP) Signatures
- ☑ Immediately Revoke Access Upon Termination or Role Change
- ☑ Use Unique User IDs and Enforce Session Timeouts

Technical

- ☑ Enforce Unique User IDs and Strong Passwords
- ☑ Enable Multi-Factor Authentication (MFA)
- ☑ Set Automatic Session Timeouts
- ☑ Restrict Access Based on Role and Need
- ☑ Log and Monitor System Activity
- ☑ Use SIEM or Alerting Tools for Threat Detection
- ☑ Protect Data Integrity with Hashing and Version Control
- ☑ Encrypt ePHI In Transit and At Rest
- ☑ Require VPNs for Remote Access

Physical

- ☑ Restrict Facility Access with Badge or Keycard Systems
- ☑ Use Video Surveillance and Access Alerts
- ☑ Require Dual Authentication for Server Room Access
- ☑ Implement Environmental Protections
- ☑ Position Workstations to Minimize Viewing Risk
- ☑ Set Automatic Screen Lock Timers
- ☑ Enforce a Clean Desk Policy
- ☑ Track and Encrypt Portable Devices and Media
- ☑ Use HIPAA-Compliant Disposal Methods