HIPAA
SELF ASSESSMENT

experts@cenovacyber.com
www.cenovacyber.com

HIPAA Safeguards Checklist – This is intended to be a quick review of your HIPAA compliance and does not replace a proper risk assessment.

Instructions: For each item, check the appropriate box and add any notes.
Scoring: Yes = 2 pts | Partial = 1 pt | No = 0 pts

Administrative Safeguards

Control	Yes -2	Partial - 1	No - 0
Risk analysis completed within the last 12 months	☐	☐	☐
Security Plan documented and approved by leadership	☐	☐	☐
Risk management program in place	☐	☐	☐
Documented security policies and procedures	☐	☐	☐
Annual HIPAA security awareness training	☐	☐	☐
Sanction policy for workforce violations	☐	☐	☐
Business Associate Agreements (BAAs) in place	☐	☐	☐
Assigned security officer	☐	☐	☐
Workforce access reviews performed regularly	☐	☐	☐
Control of all shadow IT	☐	☐	☐

Physical Safeguards

Control	Yes -2	Partial - 1	No - 0
Facility access controls implemented	☐	☐	☐
Workstation security controls enforced	☐	☐	☐
Clean desk policy for PHI	☐	☐	☐
Secure disposal of paper/electronic media	☐	☐	☐
Device and media controls enforced	☐	☐	☐
Facility access logs maintained	☐	☐	☐
Environmental controls implemented	☐	☐	☐

Technical Safeguards

Control	Yes -2	Partial - 1	No - 0
Unique user IDs for all access	☐	☐	☐
Access controls for all systems	☐	☐	☐
Monitoring and tracking of all changes	☐	☐	☐
Multi-factor authentication (MFA) enforced	☐	☐	☐
Least privilege access controls	☐	☐	☐
Encryption of ePHI at rest and in transit	☐	☐	☐
Audit logging enabled	☐	☐	☐
Regular review of logs	☐	☐	☐
Automatic session timeout	☐	☐	☐
Integrity controls in place	☐	☐	☐
Systems and Data backup plan implemented	☐	☐	☐
Disaster Recovery Plan and Testing	☐	☐	☐

Monitoring & Detection

Control	Yes -2	Partial - 1	No - 0
Centralized logging (SIEM & MDR)	☐	☐	☐
Continuous monitoring of systems	☐	☐	☐
Detection of unauthorized access	☐	☐	☐
Real-time alerting	☐	☐	☐
Defined escalation procedures	☐	☐	☐
24/7 monitoring capability	☐	☐	☐
ePHI Access monitoring and audit	☐	☐	☐
Security controls evaluated	☐	☐	☐
Vulnerability management program implemented	☐	☐	☐

Incident Response & Breach Notification

Control	Yes -2	Partial - 1	No - 0
Incident response plan documented	☐	☐	☐
Incident response testing and training in place	☐	☐	☐
Incidents logged and tracked	☐	☐	☐
Breach notification procedures (≤ 60 days)	☐	☐	☐
Roles and responsibilities defined	☐	☐	☐
Post-incident review process	☐	☐	☐

HIPAA Readiness & Updates

Control	Yes -2	Partial - 1	No - 0
Policies reviewed annually	☐	☐	☐
BAAs reviewed annually	☐	☐	☐
Supplier risk management program	☐	☐	☐
Patient data access procedures in place	☐	☐	☐
Data retention/disposal policies defined	☐	☐	☐

Add the total of each column

TOTAL _____ _____ _____

Anything less than **98 total points** means there is still some work to do. HIPAA compliance takes a significant effort to implement but once in place, the maintenance takes less effort.

This is intended to be a quick checkup for you to see where your HIPAA compliance program is. Contact us at Cenovacyber.com to schedule a free review to discuss your program and the best ways to remediate and manage it.

www.cenovacyber.com