CENOVA CYBER
MANAGED SECURITY SERVICES

www.cenovacyber.com

HIPAA Risk Assessment Quality Checklist

"Would This Hold Up Under OCR Review?"

Governance & Documentation

- ☐ Risk assessment is **written, dated, and approved**
- ☐ Methodology is clearly defined and repeatable
- ☐ Evidence retained for 6+ years
- ☐ Updated after major IT, vendor, or operational changes [hhs.gov], [feldesman.com]

Scope & ePHI Coverage

- ☐ All systems creating, receiving, storing, or transmitting ePHI included
- ☐ Email, access control, storage, backups, cloud platforms, endpoints explicitly covered
- ☐ Current technology asset inventory exists
- ☐ Network/data flow mapping documented [hhs.gov], [afslaw.com]

Threat & Vulnerability Identification

- ☐ Ransomware, phishing, access misuse, and misconfiguration assessed
- ☐ Administrative and process risks included
- ☐ Cloud and remote-access risks identified [govinfosecurity.com], [sequoia.com]

Risk Scoring & Prioritization

- ☐ Likelihood and impact defined for each risk
- ☐ Scoring logic documented
- ☐ High-risk items clearly identifiable [hhs.gov]

Risk Management & Follow-Through

- ☐ Remediation plans documented
- ☐ Risk register maintained
- ☐ Owners and timelines assigned
- ☐ Evidence of progress or resolution maintained [hipaajournal.com]

Continuous Monitoring

- ☐ Triggers defined for reassessment
- ☐ Monitoring for access, configuration, and security events
- ☐ Evidence of interim updates between annual reviews [sequoia.com], [hhs.gov]

Vendor & Business Associate Risk

- ☐ Vendors handling ePHI included
- ☐ Risk-based tiering applied
- ☐ Security expectations documented beyond BAAs [changeflow.com], [nixonpeabody.com]

See next page for scoring

CENOVA CYBER
MANAGED SECURITY SERVICES

www.cenovacyber.com

HIPAA Risk Assessment Maturity Score

Count how many boxes are checked. Each check equals one point.

🟢 Green – Defensible *(21-25 points)*

- Asset-based, documented, current
- Risks scored and actively managed
- Continuous monitoring in place
- Vendor risk included

Likely to withstand OCR review [hhs.gov]

🟡 Yellow – Partially Defensible *(15-20 points)*

- Annual assessment exists but lacks depth
- Limited monitoring between assessments
- Risk remediation informal or inconsistent
- Vendors minimally reviewed

Often triggers OCR corrective action plans [wilsonelser.com], [afslaw.com]

🔴 Red – High Enforcement Risk *(< 14 points)*

- Risk assessment missing, outdated, or generic
- No asset inventory or data flow mapping
- Risks identified but not remediated
- Vendors excluded entirely

Consistently cited in OCR enforcement actions [feldesman.com], [govinfosecurity.com]

Contact Cenova Cyber for a 30-Minute Executive Review of your results

www.cenovacyber.com