HIPAA Compliance Checklist

Use this quick-reference checklist to spot gaps, reduce risk, and stay audit-ready. ✓

Security Risk Analysis (Required)

- ☐ Have you completed a comprehensive Security Risk Analysis in the past 12 months?
- ☐ Did the analysis include physical, administrative, and technical safeguards?
- ☐ Are identified risks documented with a mitigation plan?

Administrative Safeguards

- ☐ Do you have a designated HIPAA Compliance Officer?
- ☐ Are all staff trained on HIPAA annually (and upon hiring)?
- ☐ Is there a documented contingency plan for data breaches or system failures?
- ☐ Do you conduct regular risk management reviews and audits?

Technical Safeguards

- ☐ Is data encrypted at rest and in transit?
- ☐ Do systems use role-based access controls and automatic log-offs?
- ☐ Are audit logs enabled and monitored?
- ☐ Do you use multi-factor authentication for remote access?

Physical Safeguards

- ☐ Are access controls in place for facilities where ePHI is stored?
- ☐ Are workstations secured from unauthorized access?
- ☐ Are devices that store PHI properly disposed of or wiped when retired?

HIPAA Compliance Checklist

Policies & Documentation

- ☐ Do you have written HIPAA Privacy and Security policies?
- ☐ Are Business Associate Agreements in place and current?
- ☐ Is there a process for reporting, investigating, and responding to security incidents?

Modern Compliance Essentials

- ☐ Are you using HIPAA-compliant texting, email, or telehealth platforms?
- ☐ Do you perform regular vulnerability scans and penetration testing?
- ☐ Have you tested your incident response plan in the past year?

How Did You Score?

15–20 checks: Solid footing—let's talk fine-tuning.
9–14 checks: Room to grow—let us help you close the gaps.
0–8 checks: You're at risk—schedule a free consultation.
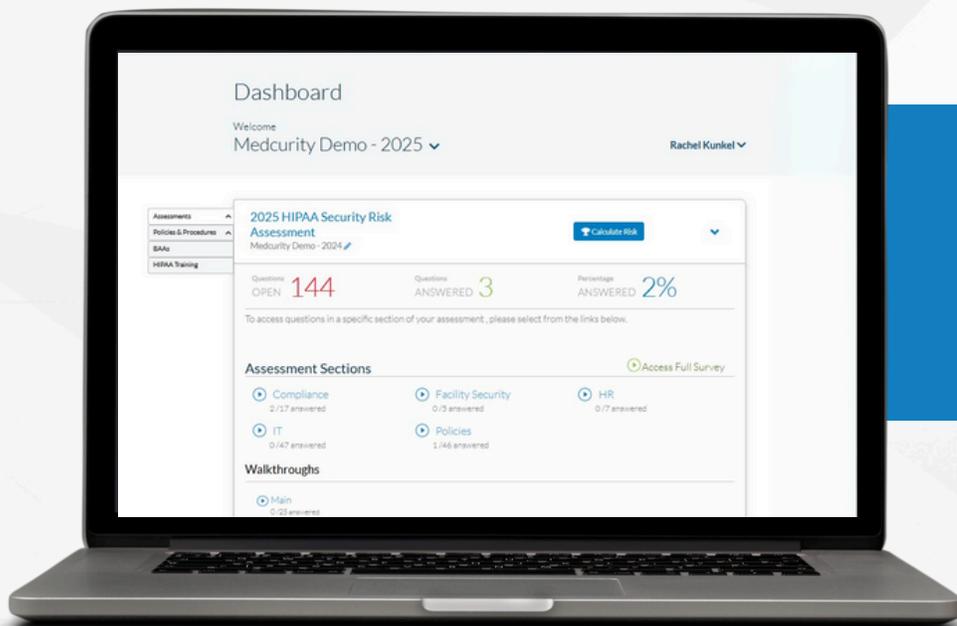
Contact Medcurity for a Quote Today!

medcurity.com
509-867-3645