

Criteria	What to Look For	Status	Notes
<b>1. Healthcare Expertise</b>	Familiarity with EHR platforms (Epic, Oracle Health, athenahealth), PACS, HL7 interfaces, clinical workflows, and legacy medical device constraints. Answers operational questions without prompting.	<input type="checkbox"/> <b>Met</b> <input type="checkbox"/> <b>Partial</b> <input type="checkbox"/> <b>Not Met</b>	
<b>2. Methodology</b>	Uses NIST CSF or HIPAA Security Rule framework. Covers all three safeguard categories: technical, administrative, physical. Assessment scoped and scaled to practice size and complexity. Methodology document available on request.	<input type="checkbox"/> <b>Met</b> <input type="checkbox"/> <b>Partial</b> <input type="checkbox"/> <b>Not Met</b>	
<b>3. Reporting Quality</b>	Executive summary with prioritized risks and recommended actions. Remediation guidance specific enough for your IT team to act on. Sample report available from a comparable healthcare client.	<input type="checkbox"/> <b>Met</b> <input type="checkbox"/> <b>Partial</b> <input type="checkbox"/> <b>Not Met</b>	
<b>4. Post-Assessment Support</b>	Remediation planning assistance included or available. Willing to answer questions during implementation. Follow-up assessment offered at defined cost. Support scope confirmed in writing before engagement.	<input type="checkbox"/> <b>Met</b> <input type="checkbox"/> <b>Partial</b> <input type="checkbox"/> <b>Not Met</b>	
<b>5. Track Record</b>	Assessors hold CISSP, CISA, or HCISPP credentials. Healthcare client references available from comparable organizations. References speak specifically to remediation guidance quality and accuracy of findings.	<input type="checkbox"/> <b>Met</b> <input type="checkbox"/> <b>Partial</b> <input type="checkbox"/> <b>Not Met</b>	