DENTAL CYBER INSURANCE READINESS

12
CONTROLS

Score every control using current evidence: 0 = missing, 1 = present but unverified, 2 = verified across the intended scope with exceptions documented. This is an educational readiness score, not an insurer rating or coverage decision.

#	CONTROL	EVIDENCE TO LOCATE	SCORE
01	**Risk analysis**	Current risk analysis, asset inventory and remediation plan	☐ 0 ☐ 1 ☐ 2
02	**Multifactor authentication**	Coverage report for remote, admin, email, cloud and backup access	☐ 0 ☐ 1 ☐ 2
03	**Endpoint protection**	Central coverage report, alerts and remediation records	☐ 0 ☐ 1 ☐ 2
04	**Patching and vulnerabilities**	Patch report, scan summary and approved exceptions	☐ 0 ☐ 1 ☐ 2
05	**Protected backups**	Encryption, separation, retention and recent restore-test proof	☐ 0 ☐ 1 ☐ 2
06	**Individual access**	User list, admin roster and access-review records	☐ 0 ☐ 1 ☐ 2
07	**Secure remote access**	Approved access, MFA, firewall evidence and no open RDP	☐ 0 ☐ 1 ☐ 2
08	**Email and training**	Filtering, SPF/DKIM/DMARC, training and phishing-test results	☐ 0 ☐ 1 ☐ 2
09	**Encryption**	Device, backup, email and transmission protection evidence	☐ 0 ☐ 1 ☐ 2
10	**Logging and monitoring**	Log sources, retention, alert routing and response tickets	☐ 0 ☐ 1 ☐ 2
11	**Incident response**	Written plan, contacts, tabletop test and continuity procedures	☐ 0 ☐ 1 ☐ 2
12	**Vendor oversight**	Vendor inventory, BAAs where required and controlled access	☐ 0 ☐ 1 ☐ 2

Total: ____ / 24 20–24 stronger evidence package 13–19 verify documentation 0–12 address major gaps

YOUR EVIDENCE PLAN

For every control, record the owner, review cadence, systems covered, evidence location and open gaps. Avoid sending sensitive technical data until your broker or counsel confirms what is needed and how it should be transferred.

CONTROL / OWNER	LATEST EVIDENCE	OPEN GAP / NEXT ACTION

Questions for the broker or carrier

1. Which controls apply to all users versus privileged or remote users?
2. How does the application define MFA, EDR, encryption and offline or immutable backup?
3. What changes must be reported during the policy term?
4. Which response vendors or counsel must be contacted first?
5. What documentation may be requested after an incident?

This educational worksheet is not legal, compliance or insurance advice. Legend Networking does not determine coverage or complete insurance applications on behalf of a practice.