Texas Dental Practice Cybersecurity Checklist

START HERE Assign an owner, mark each verified control and record the evidence - not just a yes/no answer.

1 Security risk analysis
Document where ePHI is created, stored, accessed and transmitted; prioritize remediation.

2 Complete asset inventory
Track servers, workstations, imaging devices, cloud apps, network gear and unsupported systems.

3 Multifactor authentication
Protect email, remote access, backups, administration, financial apps and vendor portals.

4 Least-privilege access
Approve access by role; review administrator rights and remove former users immediately.

5 Managed endpoint security
Confirm who investigates alerts, who can isolate devices and what happens after hours.

6 Patching and vulnerabilities
Update supported systems and document compensating controls for restricted clinical devices.

7 Secure email and network
Filter email, segment networks, separate guest Wi-Fi and control every remote-access tool.

8 Protected, tested backups
Maintain isolated encrypted copies and prove that PMS, imaging and shared data can be restored.

9 Vendor and BAA oversight
Inventory vendors, access methods, security responsibilities, agreements and offboarding steps.

10 Dental-specific training
Practice phishing, fake vendor calls, misdirected PHI and suspicious-login reporting.

11 Written incident response
Define technical, legal, insurance, communications and patient-care responsibilities.

12 Tabletop and recovery test
Run a realistic outage exercise; document gaps, decisions, recovery time and next actions.

PRIORITY REMEDIATION

Record the three gaps that should be addressed first.

1 _____ OWNER _____ DATE ____

2 _____ OWNER _____ DATE ____

3 _____ OWNER _____ DATE ____

IF AN INCIDENT OCCURS

Activate the plan | Contain carefully | Preserve evidence | Contact counsel and insurance | Document decisions

Do not label an event a reportable breach until the facts and applicable requirements have been evaluated.

Ready to test your practice? legendnt.com