

Dental IT Provider Vetting Guide

How to evaluate dental IT companies and avoid providers who don't understand your practice

- ✓ Dental-specific certifications and competencies explained
- ✓ HIPAA compliance requirements your IT provider must meet
- ✓ 10 red flags that indicate an unqualified dental IT provider
- ✓ Sample vetting questionnaire you can send to providers

What Makes Dental IT Different

Dental practices are not generic small businesses. Your IT provider must understand dental-specific practice management software (Dentrix, Eaglesoft, Open Dental), imaging systems (CBCT, panoramic, intraoral sensors), HIPAA compliance requirements unique to dental, and the clinical workflow constraints of a practice that cannot afford downtime during patient care.

Dental IT Competency Requirements

Competency Area	What It Means	Why It Matters
Practice management software	Dentrix, Eaglesoft, Open Dental, Curve configuration and support	Your PMS is the backbone of your practice — downtime = lost revenue
Digital imaging integration	CBCT, panoramic, intraoral sensor setup, DICOM/TWAIN protocols	500-700MB CBCT scans stress networks; misconfigurations lose images
HIPAA compliance	SRA, access controls, encryption, BAAs, breach notification	HIPAA violations carry fines of \$100-\$50,000 per violation (annual cap \$2M)
Dental-specific networking	Cat6 cabling per operator, imaging bandwidth, sensor compatibility	Consumer-grade networking cannot handle dental imaging traffic
Backup & disaster recovery	Encrypted offsite backup, tested restoration, ransomware protection	Dental practices are high-value ransomware targets (PHI + insurance data)

The Dental IT Litmus Test

Ask any prospective IT provider: "What's the difference between Dentrix and Eaglesoft, and how does their server architecture differ?" If they can't answer this immediately, they don't have dental practice experience.

Certifications & Credentials to Look For

IT Industry Certifications

Certification	Issuing Body	What It Proves	Relevance to Dental
CompTIA A+	CompTIA	Hardware and OS troubleshooting fundamentals	Baseline — all technicians should hold this
CompTIA Network+	CompTIA	Networking infrastructure, troubleshooting, security	Essential for imaging network design
CompTIA Security+	CompTIA	Cybersecurity fundamentals, risk management	HIPAA security baseline management
Microsoft 365 Certified	Microsoft	Cloud services, email, Teams administration	Relevant for cloud-based practices
Cisco CCNA	Cisco	Network design, routing, switching, security	Valuable for multi-site DSOs
HIPAA Compliance Officer (CHPS)	AHIMA	Healthcare privacy and security expertise	Gold standard for HIPAA compliance

Vendor-Specific Credentials

Credential	Vendor	What It Means
Dentrix Certified Trainer	Henry Schein	Authorized to train and support Dentrix
TechCentral Certified	Henry Schein	Certified dental IT provider through Henry Schein's program
Eaglesoft Certified	Patterson Dental	Authorized for Eaglesoft support and configuration
Dexis Certified Installer	Dexis	Qualified for imaging sensor installation and integration
SonicWall Partner	SonicWall	Certified for firewall and network security deployment

The minimum bar

Your dental IT provider should have CompTIA-certified technicians, HIPAA compliance expertise (not just marketing claims), and documented experience with your specific practice management software. Vendor-specific dental certifications (TechCentral, Eaglesoft Certified) are strong signals.

HIPAA Compliance: What Your IT Provider Must Do

HIPAA Requirements Your IT Provider Is Responsible For

Under the HIPAA Security Rule, your IT provider is a Business Associate who must sign a BAA and meet specific security requirements. The 2025 HIPAA Security Rule updates introduced stricter requirements that many dental IT providers have not yet implemented.

Required HIPAA Technical Safeguards

Requirement	What It Means	IT Provider Responsibility
Unique user IDs	Every staff member has their own login — no shared accounts	Configure individual accounts on all systems
Multi-factor authentication (MFA)	Second verification factor for all PHI access	Enable and enforce MFA on PMS, imaging, email, remote access
Encryption at rest and in transit	All PHI encrypted on hard drives and during transmission	Full-disk encryption, TLS for email, VPN for remote access
Access controls	Role-based permissions; minimum necessary access	Configure user roles in PMS, restrict admin access
Audit logging	Track who accessed what PHI and when	Enable and review audit logs in PMS and server
Security Risk Assessment (SRA)	Annual comprehensive risk evaluation	Conduct or facilitate annual SRA
Vulnerability scanning	System scans every 6 months	Run and remediate vulnerability scans
Breach notification (72 hours)	Report breaches within 72 hours (updated from 60 days)	Incident response plan with IT provider as first call
Business Associate Agreement	Signed BAA between practice and IT provider	IT provider must sign BAA before accessing any PHI

Critical

If your IT provider does not have a signed BAA with your practice, they are in violation of HIPAA — and so are you. If they cannot explain what an SRA is or when your last one was completed, replace them immediately.

10 Red Flags of an Unqualified Dental IT Provider

1 **No dental practice experience.**

Cannot name the practice management software your practice uses, has never configured a dental imaging sensor, and treats your practice like a generic small business. Dental IT is specialized — general MSPs learn on your dime.

2 **No signed BAA on file.**

A Business Associate Agreement is not optional. Any IT provider who accesses your network without a signed BAA is putting your practice at legal and financial risk.

3 **Cannot produce HIPAA compliance documentation.**

If asked for their SRA template, incident response plan, or HIPAA policy documentation, they deflect or don't have it. HIPAA compliance is not a checkbox — it's an ongoing program.

4 **Uses shared admin credentials.**

If your IT provider logs into your server with a single "admin" account shared across all their technicians, they are violating HIPAA access control requirements and making incident attribution impossible.

5 **No backup testing.**

Claims backups run nightly but cannot produce documentation of a recent test restore. Untested backups are not backups — they are assumptions.

6 **Slow response times with no SLA.**

If it takes 4+ hours to respond to a server-down incident during patient hours, your practice is losing revenue. No written SLA means no accountability.

7 **Does not understand imaging workflows.**

CBCT scans (500-700MB per study), panoramic images, and intraoral sensors require specific network bandwidth, storage architecture, and integration configuration. If your provider treats imaging like "just another file," expect data loss.

8 **Recommends consumer-grade equipment.**

If your IT provider suggests consumer WiFi routers, unmanaged switches, or Windows Home edition for your practice, they don't understand dental IT requirements.

9**No cybersecurity beyond antivirus.**

Antivirus alone is insufficient in 2026. Dental practices need managed firewall, email security, endpoint detection, staff training, and vulnerability scanning. If their "security plan" is Norton, run.

10**Provides no reporting or documentation.**

A competent MSP provides monthly reports: tickets opened/closed, response times, security events, backup status, and patch compliance. No reporting means no accountability and no basis for evaluating their performance.



When Dental-Specific Expertise Matters (Decision Matrix)

Two-column layout

REQUIRE DENTAL-SPECIALIZED IT WHEN

- Practice uses Dentrix, Eaglesoft, or other dental-specific PMS
- Practice has CBCT, panoramic, or digital intraoral sensors
- Practice needs HIPAA compliance management (all practices)
- New office build-out with dental-specific cabling requirements
- Migration between practice management systems
- DSO with multiple locations requiring standardized IT
- Practice has experienced a data breach or ransomware incident

GENERAL MSP MAY SUFFICE WHEN

- Practice uses only cloud-native software (Curve, Dentrix Ascend) with no on-premise server
- IT needs are limited to email, internet, and basic workstations
- Practice has an internal "tech-savvy" office manager for day-to-day issues
- Even here: verify HIPAA compliance capability and get a signed BAA

Cost comparison

Factor	Dental-Specialized MSP	General MSP
Monthly managed services	\$500-\$2,500/mo	\$300-\$1,500/mo
Imaging support	Included or clear add-on pricing	Hourly at \$150-\$250/hr (learning curve)
HIPAA compliance	Built into service model	Often an add-on or outsourced
PMS support	In-house expertise	Escalates to PMS vendor (delays)
Response time for dental-specific issues	15-60 minutes (knows the systems)	2-4 hours (research time)
New office build-out	Turnkey (cabling through imaging)	Subcontracts dental-specific work

Sample Vetting Questionnaire

Dental IT Provider Vetting Questionnaire — Send This Before Hiring

Copy and send these questions to any dental IT provider or MSP you're considering. Their answers will tell you everything you need to know.

1. Dental Experience

- How many dental practices do you currently support?
- Which practice management systems do you have experience with (Dentrix, Eaglesoft, Open Dental, Curve)?
- Have you integrated CBCT imaging systems? Which brands (Carestream, Planmeca, Dexis, Sirona)?
- Do you have Dentrix/Eaglesoft certified technicians on staff?

2. HIPAA Compliance

- Do you provide annual HIPAA Security Risk Assessments? Can you share a sample report?
- What is your process for BAA execution with your clients?
- How do you handle breach notification and incident response?
- Do you conduct vulnerability scanning? How frequently?
- How do you enforce MFA and access controls across practice systems?

3. Service Level & Support

- What is your average response time for critical issues (server down, unable to access patient records)?
- Do you provide written SLAs with response and resolution time guarantees?
- What are your after-hours/emergency support procedures and rates?
- How many technicians do you have available for on-site support in our area?
- Do you provide a dedicated account manager or point of contact?

4. Backup & Security

- What is your backup strategy (frequency, location, encryption)?
- When was the last time you performed a full test restore for a dental client?
- What cybersecurity tools do you deploy (firewall, endpoint detection, email security, training)?
- Do you provide ransomware-specific protection and incident response?

- What cyber insurance do you carry?

5. Pricing & Contracts

- What is your pricing model (per-device, per-user, flat fee)?
- What is and isn't included in your monthly fee? Can you provide a written service catalog?
- What are your after-hours and on-site visit rates?
- What is the contract term and cancellation policy?
- Do you markup hardware? What is your pricing model for equipment purchases?
- What is included during the transition/onboarding period?

6. References

- Can you provide 3 references from dental practices of similar size to ours?
- Can you share a sample monthly report?

HIPAA Compliance Quick-Reference Card

HIPAA Compliance Checklist for Dental Practices — Tear Out and Post

Administrative Safeguards

- ☐ Designated HIPAA Privacy Officer and Security Officer
- ☐ Annual Security Risk Assessment (SRA) completed and documented
- ☐ Written HIPAA policies and procedures (updated annually)
- ☐ All staff trained on HIPAA (at hire + annually)
- ☐ Business Associate Agreements signed with all vendors who access PHI
- ☐ Incident response plan documented and tested

Technical Safeguards

- ☐ Unique user IDs on all systems (no shared logins)
- ☐ Multi-factor authentication enabled on all PHI-accessing systems
- ☐ Full-disk encryption on all workstations, laptops, and servers
- ☐ Email encryption for any PHI transmitted electronically
- ☐ Firewall and intrusion detection active and monitored
- ☐ Vulnerability scanning completed every 6 months
- ☐ Automatic session timeout on all workstations (15 minutes)

Physical Safeguards

- ☐ Server room locked with restricted access
- ☐ Workstation screens not visible to patients

☐ Printed PHI secured in locked storage

☐ Devices containing PHI tracked in asset inventory

☐ Disposal procedures for old hard drives (NIST 800-88 wipe or physical destruction)

ChairsideIT

ChairsideIT

IT support built for dental practices.

[Browse providers at chairsideit.com](https://chairsideit.com)