

HIPAA Compliance Checklist for Dental Practices

25-point technical safeguards audit based on HIPAA Security Rule (45 CFR §164.312). Use this checklist to evaluate your practice's security posture and identify gaps before your next risk assessment.

Access Controls (§164.312(a))

- 1 Every staff member has a unique login — no shared accounts for Dentrix, Eaglesoft, or workstations.
- 2 Role-based access is configured — front desk cannot access clinical notes, hygienists cannot access billing.
- 3 Automatic screen lock activates after 5 minutes of inactivity on all workstations.
- 4 Multi-factor authentication (MFA) is enabled on email, cloud apps, and remote access.

Audit Controls (§164.312(b))

- 5 Login attempts and access to patient records are logged and retained for 6+ years.
- 6 Audit logs are reviewed at least quarterly for unusual access patterns.
- 7 Failed login attempts trigger alerts to your IT administrator.

Integrity Controls (§164.312(c))

- 8 Anti-tamper protections are in place for electronic patient records.
- 9 Digital X-ray files (DICOM) are stored on encrypted, access-controlled storage.
- 10 Database integrity checks run automatically on practice management software.

Person or Entity Authentication (§164.312(d))

- 11 Passwords meet minimum complexity requirements (12+ characters, no dictionary words).
- 12 Terminated employees are deprovisioned within 24 hours across all systems.
- 13 Vendor access (Dentrix support, IT provider) uses temporary, audited credentials.

Transmission Security (§164.312(e))

- 14 Patient data is encrypted in transit (TLS 1.2+) for email, cloud sync, and remote access.
- 15 Encrypted email or secure portal is used for sending patient information externally.
- 16 Wi-Fi networks use WPA3 or WPA2-Enterprise with separate guest and clinical networks.

Device & Endpoint Security

- 17 All workstations run endpoint detection and response (EDR) — not just basic antivirus.

18 Full-disk encryption (BitLocker/FileVault) is enabled on every device with patient data.

19 X-ray workstations and imaging servers are on isolated network segments.

Network Security

20 Business-class firewall with intrusion detection is in place (not a consumer router).

21 Network segmentation separates clinical systems, front office, and guest Wi-Fi.

Backup & Disaster Recovery

22 Automated daily backups with at least one off-site or cloud copy (3-2-1 rule).

23 Backup restoration is tested at least quarterly to verify recoverability.

Documentation & Training

24 Written HIPAA Security Risk Assessment completed and staff security training documented within the last 12 months.

25 All staff complete HIPAA security awareness training annually with documented sign-off.

Red Flags — Get Professional Help Immediately

If any of these apply to your practice, contact a security professional before your next audit:

- Shared logins across staff ("everyone uses the same Dentrix password")
- No encryption on workstations or laptops that leave the office
- Patient data sent via regular (unencrypted) email
- No written risk assessment on file — this is the #1 HIPAA audit finding
- X-ray or imaging systems running unsupported Windows versions (Windows 7/XP)
- No backup testing — backups exist but have never been verified
- Consumer-grade router with no firewall logging or intrusion detection

Ready to Secure Your Practice?

Get a free security assessment — no obligation, no sales pitch.

(469) 306-9520 | pdgeek.com/contact

This checklist is for informational purposes only and does not constitute legal advice. HIPAA compliance requires a formal risk assessment conducted by a qualified professional. © 2026 Pleasant Digital LLC (PD Geek). All rights reserved.