QUADRAPAY MERCHANT SERVICES CONSULTANCY

INTERACTIVE CHECKLIST

HIPAA & PCI Compliance Checklist

For dental practices accepting card payments — check off each item as you confirm it with your payment processor and internal team.

A. DATA SECURITY & ENCRYPTION

- ☐ Card data is encrypted in transit and at rest (end-to-end / point-to-point encryption)
- ☐ Card numbers are tokenized rather than stored in your practice management system
- ☐ Payment terminals and gateway are PCI DSS validated
- ☐ Patient payment data is never emailed, texted, or stored in plain text
- ☐ Card-on-file storage for recurring billing uses a secure vault, not raw card numbers

B. HIPAA-SPECIFIC SAFEGUARDS

- ☐ Payment processor confirms it does not access or store protected health information (PHI)
- ☐ A signed Business Associate Agreement (BAA) is in place if the processor could touch PHI
- ☐ Payment confirmations / receipts do not disclose treatment details or diagnosis codes
- ☐ Patient financing partner (if used) has its own written data-handling policy on file

C. STAFF & ACCESS CONTROLS

- ☐ Front-desk staff are trained on secure card handling and phishing awareness
- ☐ Access to the payment portal / terminal is role-based, not shared logins
- ☐ Staff offboarding includes immediate removal of payment-system access

INTERACTIVE CHECKLIST

Incident Readiness & Vendor Diligence

Confirm your practice is ready if something goes wrong, and every vendor in the payment chain meets the bar.

D. INCIDENT & CHARGEBACK READINESS

- [ ] Written procedure exists for reporting a suspected data breach
- [ ] Processor provides 24/7 support for fraud alerts and disputed transactions
- [ ] Chargeback response process and documentation (signed consent, treatment records) is defined
- [ ] Practice knows its current chargeback rate and what triggers high-risk review

E. VENDOR & SOFTWARE DILIGENCE

- [ ] Practice management software integration (Dentrix / Eaglesoft / Open Dental / other) is PCI-aware
- [ ] Online patient payment portal uses HTTPS and a PCI-compliant hosted payment page
- [ ] Any third-party financing or online booking tool handling card data is separately vetted
- [ ] Annual PCI self-assessment questionnaire (SAQ) is completed and on file

Open items / follow-ups: