



Dental IT & HIPAA Readiness Checklist

A plain-English self-check for independent dental practices

Practice

Completed by

Date

IT provider / contact

How to use it

For each item, mark Yes, Partly, No, or Not sure. "Not sure" is useful—it identifies where ownership or visibility is missing. Prioritize items tied to patient care, recovery, privileged access, and unsupported systems.

This checklist is educational and high-level. It is not legal advice, a compliance certification, or a formal HIPAA Security Risk Analysis. HIPAA obligations depend on your actual environment, policies, vendors, and operations.

1. Inventory & ownership

Readiness question	Yes	Partly	No	Not sure
A1 We maintain a current inventory of workstations, servers, network devices, and clinical technology.	☐	☐	☐	☐
A2 Every critical system and vendor has a named internal owner and current support contact.	☐	☐	☐	☐
A3 We know which devices or operating systems are approaching end of support.	☐	☐	☐	☐
A4 Network diagrams, admin credentials, warranties, and key configurations are documented securely.	☐	☐	☐	☐

2. Accounts & access

Readiness question	Yes	Partly	No	Not sure
B1 Each team member uses an individual account rather than a shared login.	☐	☐	☐	☐
B2 Multi-factor authentication is enabled for email, remote access, cloud services, and administrator accounts.	☐	☐	☐	☐
B3 Administrator access is limited and separate from routine daily accounts.	☐	☐	☐	☐
B4 Access is removed promptly when an employee or vendor no longer needs it.	☐	☐	☐	☐
B5 Remote access is approved, documented, encrypted, and reviewed regularly.	☐	☐	☐	☐

3. Workstations & servers

Readiness question	Yes	Partly	No	Not sure
C1 Supported operating systems and business applications receive security updates on a defined schedule.	☐	☐	☐	☐
C2 Managed endpoint protection is installed, monitored, and able to alert someone who will respond.	☐	☐	☐	☐
C3 Workstations lock automatically and require a user to authenticate again.	☐	☐	☐	☐
C4 USB storage and local administrator rights are controlled based on business need.	☐	☐	☐	☐
C5 Servers and key workstations have enough capacity and warranty coverage for practice operations.	☐	☐	☐	☐

4. Network, firewall & Wi-Fi

Readiness question	Yes	Partly	No	Not sure
D1 The firewall is business-grade, supported, patched, and configured by a qualified administrator.	☐	☐	☐	☐
D2 Guest Wi-Fi is separated from clinical systems, staff devices, servers, and equipment.	☐	☐	☐	☐
D3 Network access is segmented where appropriate for imaging, clinical devices, phones, and business systems.	☐	☐	☐	☐
D4 Internet outages have a documented response or failover plan appropriate to the practice.	☐	☐	☐	☐
D5 Firewall, switch, access-point, and ISP credentials are documented securely and recoverable.	☐	☐	☐	☐

5. Backup & recovery

Readiness question	Yes	Partly	No	Not sure
E1 Backups cover servers, practice-management data, imaging data, and other critical systems.	☐	☐	☐	☐
E2 At least one protected backup copy is isolated from routine user and administrator access.	☐	☐	☐	☐
E3 Backup failures are monitored and assigned to someone for prompt follow-up.	☐	☐	☐	☐
E4 A full or representative restore has been tested and documented within the last 12 months.	☐	☐	☐	☐
E5 The practice knows its acceptable downtime and data-loss limits for critical systems.	☐	☐	☐	☐

6. Email & communication

Readiness question	Yes	Partly	No	Not sure
F1 Email accounts use MFA and modern spam, phishing, and malicious-link protection.	☐	☐	☐	☐
F2 The practice has a method to identify suspicious payment, payroll, and account-change requests.	☐	☐	☐	☐
F3 Sensitive information is shared through approved secure methods rather than ordinary email when appropriate.	☐	☐	☐	☐
F4 Team members receive practical security awareness guidance and know how to report suspicious messages.	☐	☐	☐	☐

7. Dental systems & vendors

Readiness question	Yes	Partly	No	Not sure
G1 Practice-management, imaging, payment, lab, and equipment dependencies are documented.	☐	☐	☐	☐
G2 Vendor remote access is limited, approved, and disabled or reviewed when not needed.	☐	☐	☐	☐
G3 A single person or provider coordinates issues that cross dental software, hardware, network, and internet vendors.	☐	☐	☐	☐
G4 Upgrades to Dentrix, Eaglesoft, Open Dental, Curve Dental, Practice-Web, imaging, or equipment are planned and tested.	☐	☐	☐	☐
G5 Business associate agreements are tracked for vendors that may handle protected health information.	☐	☐	☐	☐

8. HIPAA readiness & documentation

Readiness question	Yes	Partly	No	Not sure
H1 The practice has a current, documented HIPAA Security Risk Analysis appropriate to its environment.	☐	☐	☐	☐
H2 Security policies, sanctions, contingency procedures, and workforce responsibilities are documented and reviewed.	☐	☐	☐	☐
H3 Required HIPAA/security training is completed and documented.	☐	☐	☐	☐
H4 Technology risks and remediation decisions are tracked, assigned, and reviewed by leadership.	☐	☐	☐	☐
H5 The practice retains documentation supporting safeguards, training, incidents, and vendor oversight.	☐	☐	☐	☐

9. Incident readiness

Readiness question	Yes	Partly	No	Not sure
I1 The team knows who to contact first for suspected ransomware, account compromise, data exposure, or equipment theft.	☐	☐	☐	☐
I2 An incident-response plan defines immediate containment, communication, documentation, and recovery steps.	☐	☐	☐	☐
I3 Cyber-insurance contact details and policy requirements are available before an incident.	☐	☐	☐	☐
I4 Emergency contact details for IT, leadership, legal counsel, insurance, and key vendors are current.	☐	☐	☐	☐
I5 The response plan has been discussed or tested with a tabletop exercise during the last 12 months.	☐	☐	☐	☐

Your five highest-priority gaps

Choose the items most likely to interrupt patient care, expose sensitive information, block recovery, or leave a critical system without an owner.

Priority	Gap / concern	Owner	Target date
1			
2			
3			
4			
5			

Want a second set of eyes?

Book a free 15-minute Dental IT Risk Review. No remote access is required for the introductory call. We will help you decide what can stay as-is, what deserves attention, and whether a deeper assessment makes sense.

brotherlytechnology.com/dental-practices-request-consultation/
404-907-1005 · hello@brotherlytechnology.com