

DENTAL IT CHECKLIST

The Dental Practice IT Checklist

Built around the way a practice actually runs - imaging, practice management, and the HIPAA obligations that come with both.

01	Imaging and PMS backup requirements most practices miss
02	HIPAA technical safeguards for a small practice
03	What to fix before your next operatory goes down

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology

Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

☐ Practice-management and imaging systems have named owners, versions, vendors, and support status.	☐ Yes ☐ Partial ☐ No
☐ Every ePHI location is included in the data map and backup scope.	☐ Yes ☐ Partial ☐ No
☐ Image and database backups are application-consistent and monitored.	☐ Yes ☐ Partial ☐ No
☐ A restore test opens patient records and diagnostic images in a supported application.	☐ Yes ☐ Partial ☐ No
☐ Workstations use unique accounts, least privilege, encryption, auto-lock, and managed protection.	☐ Yes ☐ Partial ☐ No
☐ MFA covers email, remote access, cloud applications, and privileged accounts.	☐ Yes ☐ Partial ☐ No
☐ Audit logging and access reviews support accountability for patient data.	☐ Yes ☐ Partial ☐ No
☐ Vendors that handle ePHI are tracked with BAAs and security contacts.	☐ Yes ☐ Partial ☐ No
☐ Clinical, guest, imaging, VoIP, and device traffic are segmented where appropriate.	☐ Yes ☐ Partial ☐ No
☐ Operatory downtime procedures cover scheduling, chart access, imaging, phones, and payment.	☐ Yes ☐ Partial ☐ No
☐ UPS capacity and safe shutdown protect critical network, server, and imaging components.	☐ Yes ☐ Partial ☐ No
☐ The practice has tested incident, ransomware, and extended-outage communications.	☐ Yes ☐ Partial ☐ No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

Protect the image, the database, and the relationship between them

A folder copy may miss an open database, configuration, license, or image index. Validate recovery with the actual applications and vendors.

System	Backup requirement	Restore proof
Practice management	Application-aware database plus configuration and documents	Open patient, appointment, ledger, and report
Imaging	Images, database/index, templates, calibration, and settings	Search patient and open representative images
Cloud PMS / imaging	Document vendor recovery plus independent export/backup decision	Export, retention, and recovery test evidence
Workstations	Standard build and critical local settings; avoid local-only ePHI	Replace a device and resume workflow
Network / firewall	Configuration export, firmware record, ISP and VPN details	Restore configuration to spare or test unit
RTO / RPO	Targets approved by practice leadership	Timed exercise with clinical validation

Ask the PMS and imaging vendors to document supported backup and restore methods. Unsupported snapshots can look complete while producing unusable data.

Keep one operator failure from stopping the practice

Combine HIPAA safeguards with practical operator readiness: standardized devices, spare capacity, clean cabling, and a paper or alternate workflow.

1	Standardize operator hardware, peripherals, software versions, labels, and cable paths.
2	Keep a tested spare workstation or rapid replacement image with required drivers and application steps.
3	Segment and document clinical devices; restrict vendor remote access to approved, logged methods.
4	Create downtime sheets for schedule, patient contact, clinical notes, imaging, prescriptions, and payments.
5	Test one operator loss and one server/internet outage during a planned window; record recovery time and fixes.

What to watch for

WATCH: Images exist in a folder backup but the imaging database was not captured consistently.

WATCH: Vendor remote access uses a shared account or remains permanently enabled.

WATCH: ePHI is stored on desktops because the supported share is slow.

WATCH: A spare workstation has never opened the PMS or imaging software.

WATCH: Clinical downtime steps depend on email or the unavailable PMS.

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: HHS HIPAA Security Rule: hhs.gov/hipaa/for-professionals/security/ | CISA Healthcare and Public Health: cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector

This guide is educational and is not legal, regulatory, tax, or insurance advice. Confirm requirements and pricing for your organization with qualified advisors and vendors.