

Dental Practice IT Setup Checklist

A step-by-step guide to building reliable, HIPAA-compliant technology for your dental practice

- ✓ New office IT infrastructure checklist (28 items)
- ✓ Network design for dental imaging and practice management
- ✓ HIPAA-compliant security configuration guide
- ✓ Software integration and go-live protocol

Phase 1: Planning & Design (8-12 Weeks Before Opening)

IT Infrastructure Planning

- ☐ Hire dental-specialized IT provider (see Vetting Guide) — do this BEFORE construction starts
- ☐ Create operatory floor plan with data drop locations for each chair
- ☐ Plan server room / IT closet location (climate-controlled, lockable, ventilated)
- ☐ Select practice management software (Dentrix, Eaglesoft, Open Dental, Curve)
- ☐ Select imaging software and verify PMS compatibility
- ☐ Determine cloud-based vs. on-premise server architecture
- ☐ Design network topology (separate VLANs for clinical, imaging, guest WiFi, VoIP)
- ☐ Specify internet service: business-class fiber (minimum 100 Mbps symmetric) + cellular backup
- ☐ Budget for IT setup (\$20,000-\$45,000 for typical 5-operator office)

Vendor Coordination

- ☐ Coordinate IT cabling with general contractor (during rough-in, before drywall)
- ☐ Schedule imaging equipment delivery and integration with IT provider
- ☐ Confirm practice management software licensing and installation timeline
- ☐ Order hardware (workstations, server, switches, firewall, WAPs, UPS) — allow 3-4 week lead time
- ☐ Coordinate phone system (VoIP) with network design

Critical

Engage your IT provider during the design phase, not after construction. Running cabling during rough-in costs \$3,500-\$5,500/operator. Retrofitting after drywall costs \$7,000-\$11,000/operator and results in surface-mounted cable runs.

Phase 2: Network Infrastructure (4-8 Weeks Before Opening)

Cabling & Core Network

- ☐ Install Cat6 (minimum) or Cat6A cabling to every operatory, front desk, and server room
- ☐ Run minimum 2 data drops per operatory (1 for workstation, 1 for imaging)
- ☐ Install additional drops for: panoramic sensor, CBCT, intraoral camera, VoIP phone
- ☐ Test all cable runs with cable tester — document results
- ☐ Install business-grade managed switches (Gigabit, PoE for WAPs and cameras)
- ☐ Install and configure HIPAA-compliant firewall (SonicWall, Fortinet, or equivalent)
- ☐ Install enterprise WiFi access points with separate SSIDs (clinical, staff, patient)

Server Room Setup

- ☐ Install server rack or wall-mount enclosure
- ☐ Verify climate control (server room should stay below 75°F / 24°C)
- ☐ Install UPS (uninterruptible power supply) — minimum 30 minutes runtime for graceful shutdown
- ☐ Connect UPS to server with shutdown monitoring cable
- ☐ Install and configure on-premise server (if required by PMS)
- ☐ Configure RAID storage for data redundancy
- ☐ Install and configure backup system (local NAS + encrypted cloud replication)

CBCT Bandwidth Planning

A single CBCT scan can be 500-700MB. If your CBCT unit is more than one switch hop from your server, image transfer will be slow. Run a dedicated Cat6A cable from the CBCT acquisition PC directly to the server switch — do not route through an operatory switch.

Phase 3: Workstation & Software Setup (2-4 Weeks Before Opening)

Workstations

- ☐ Deploy clinical workstations at each operatory (minimum specs: i5/Ryzen 5, 16GB RAM, SSD, dual monitors)
- ☐ Deploy front desk workstations (same specs + barcode scanner, check scanner if applicable)
- ☐ Deploy imaging acquisition PCs (CBCT/panoramic — dedicated machines per manufacturer specs, no other peripherals)
- ☐ Configure all workstations with Windows 11 Pro (NOT Home edition)
- ☐ Enable BitLocker full-disk encryption on all workstations
- ☐ Install and configure antivirus/endpoint detection (managed by MSP)
- ☐ Configure automatic Windows updates (staged, tested before production deployment)

Practice Management Software

- ☐ Install practice management software on server and all workstations
- ☐ Configure database with practice information, provider profiles, fee schedules
- ☐ Set up appointment scheduling templates and operatory assignments
- ☐ Configure insurance and billing modules
- ☐ Import or enter patient records (if migrating from another PMS)
- ☐ Set up user accounts with role-based permissions (NO shared logins)
- ☐ Test all workstation-to-server connections under load

Imaging Integration

- ☐ Install imaging software on server and clinical workstations

- ☐ Configure imaging software to use shared network storage path (all workstations pointing to same directory)
- ☐ Install and test intraoral sensor drivers at each operatory
- ☐ Configure panoramic unit interface and test image capture to PMS
- ☐ Configure CBCT unit interface and test scan acquisition to imaging server
- ☐ Verify image bridging between imaging software and PMS (patient records link to images)

Phase 4: Security & HIPAA Configuration (1-2 Weeks Before Opening)

Access Controls

- ☐ Create individual user accounts for every staff member on all systems
- ☐ Assign role-based permissions (provider, hygienist, front desk, billing, admin)
- ☐ Enable multi-factor authentication on PMS, email, remote access, and cloud services
- ☐ Configure automatic screen lock after 15 minutes of inactivity
- ☐ Disable USB ports on clinical workstations (prevent unauthorized data transfer)
- ☐ Configure password policy: minimum 12 characters, complexity required, 90-day rotation

Backup & Disaster Recovery

- ☐ Configure automated daily backup (full weekly + incremental daily)
- ☐ Encrypt backup data at rest and in transit (AES-256)
- ☐ Configure offsite cloud backup replication (separate from primary cloud services)
- ☐ Perform full test restore and document results
- ☐ Create and print downtime procedures (paper-based patient intake, manual scheduling)
- ☐ Store downtime kit at front desk: printed forms, pen, appointment book

Email & Communications

- ☐ Configure HIPAA-compliant email (Microsoft 365 with E3/E5 or Google Workspace with BAA)
- ☐ Enable email encryption for PHI (TLS enforcement + optional message-level encryption)
- ☐ Configure email security: anti-phishing, anti-malware, DMARC/DKIM/SPF
- ☐ Set up patient communication system (appointment reminders, recall)

- ☐ Verify all patient-facing communications comply with HIPAA (no PHI in unencrypted texts/emails)
-

Phase 5: Testing & Go-Live (Week of Opening)

System Testing

- ☐ Run full end-to-end test: schedule appointment → check in → chart → image capture → treatment plan → checkout → claim submission
- ☐ Test imaging workflow at every operator: capture → save → view in PMS
- ☐ Test CBCT scan acquisition, transfer, and viewing
- ☐ Verify all printers, scanners, and label printers function
- ☐ Test phone system (inbound, outbound, hold, transfer, voicemail)
- ☐ Verify internet speed test: confirm minimum 100 Mbps down/50 Mbps up
- ☐ Test WiFi coverage in all patient and clinical areas
- ☐ Verify backup ran successfully and test restore on one file

Staff Training

- ☐ Train all clinical staff on PMS workflows (scheduling, charting, imaging)
- ☐ Train front desk on check-in/checkout, insurance verification, payment processing
- ☐ Train all staff on HIPAA basics (PHI handling, password policy, incident reporting)
- ☐ Train all staff on cybersecurity awareness (phishing identification, social engineering)
- ☐ Post emergency IT contact information at front desk and in each operator
- ☐ Distribute quick-reference cards for common PMS tasks

Go-Live Day Rule

Have your IT provider on-site for the entire first day of patient appointments. Equipment that works in testing may behave differently under real-world load. The cost of one day of on-site support (\$500-\$1,500) is trivial compared to the cost of a chaotic first day with patients.

Network Architecture Reference Diagram

Dental Office Network Design — Reference Architecture

Visual network diagram

Design a clean network topology diagram showing:

- **Internet** → **Firewall** (SonicWall/Fortinet) → **Core Switch** (managed, Gigabit, PoE)
- Core Switch connects to:
- **Server** (on-premise, PMS + imaging database, RAID storage, UPS)
- **Operatory Switch** → Operatory workstations (x5), intraoral sensors, panoramic unit
- **CBCT Acquisition PC** (dedicated direct connection to core switch)
- **Front Desk Switch** → Reception workstations (x2), printer, scanner, check scanner
- **WiFi Access Points** (3 SSIDs: Clinical, Staff, Patient-Guest)
- **VoIP Phones** (PoE powered from switches)
- **NAS Backup** (local backup target)
- Cloud connections: offsite backup, cloud PMS (if applicable), email (M365/Google)

Color coding

- Clinical VLAN: Primary 600 (cyan)
- Staff VLAN: Emerald
- Guest WiFi VLAN: Gray
- Imaging traffic: Amber (high-bandwidth callout)

Key Design Principles

(1) Separate VLANs for clinical, staff, and guest traffic — patient WiFi should never touch clinical systems. (2) CBCT acquisition PC connects directly to core switch, not through an operatory switch — imaging traffic needs maximum bandwidth. (3) UPS on server and core switch — everything else can reboot; losing the server mid-appointment loses data.

Ongoing Maintenance Schedule

Annual IT Maintenance Calendar for Dental Practices

Frequency	Task	Who
Daily	Verify backup completion	MSP (automated monitoring)
Weekly	Review security alerts and patch status	MSP
Monthly	Review help desk tickets and response times	Office manager + MSP
Monthly	Test one random file restore from backup	MSP
Quarterly	Update firewall firmware and security policies	MSP
Quarterly	Review and update user access (terminated employees, role changes)	Office manager + MSP
Every 6 months	Vulnerability scan and remediation	MSP
Annually	Full HIPAA Security Risk Assessment	MSP + HIPAA officer
Annually	Cybersecurity awareness training for all staff	MSP or third-party
Annually	Review and update disaster recovery plan	MSP + office manager
Every 4-5 years	Workstation hardware refresh	MSP (planned budget)
Every 5-7 years	Server hardware refresh	MSP (planned budget)
As needed	Imaging sensor calibration and updates	Imaging vendor + MSP

ChairsideIT

ChairsideIT

1. ****Printability matters.**** Dental office managers print these for team meetings and vendor discussions. Avoid large solid color areas on interior pages (waste ink). Reserve full-bleed backgrounds for cover and back cover only. 2. ****Tables are the star.**** These guides live or die on their reference tables. Make tables scannable, well-spaced, and easy to read at 100% zoom on screen AND when printed

Find providers at chairsideit.com