

# MANAGED IT FOR DENTAL PRACTICES CHECKLIST



## Executive Tool for Operational Continuity & Security

Built for dental practice owners and IT decision-makers. Use this checklist to evaluate IT support, security, compliance, and reliability.



## How to Use

1. Takes 20–30 minutes
2. Check each box that applies
3. Count the total number of checked items
4. Identify cost, security, and uptime risks

1

## IT Support Model & Contracts

- Document current IT support arrangements
- Verify response time commitments in contracts
- List all support vendors and contact info
- Validate after-hours support availability
- Confirm escalation process for critical incidents
- Document support cost structure and billing

3

## Security & Compliance Controls

- Confirm HIPAA technical safeguards are applied
- Verify encryption on all patient data storage
- Audit user access controls and permissions
- Ensure multi-factor authentication is enforced
- Validate firewall and network protections
- Document compliance policies and reviews

2

## Hardware & Software Inventory

- List all computers, servers, and devices
- Record software licenses and versions
- Track EHR system dependencies
- Identify unsupported or outdated systems
- Document maintenance and replacement schedules
- Ensure antivirus/endpoint protection coverage

4

## Backup & Disaster Recovery

- Verify automated backups run daily
- Confirm backups stored off-site or in cloud
- Test data restoration within last 90 days
- Document Recovery Time Objective (RTO)
- Document Recovery Point Objective (RPO)
- Identify responsible owner for DR plan



5

## Monitoring & Maintenance

- Enable real-time monitoring for key systems
- Track uptime of computers and network
- Monitor critical application performance
- Schedule regular security patching
- Log incidents for audit and review
- Review monitoring alerts monthly

6

## Vendor Management & Roadmap

- Review third-party vendor performance
- Validate software support agreements
- Check warranty status on hardware
- Plan IT budget for next 12 months
- Identify system upgrades required
- Document IT roadmap and goals



### Scoring Model

- Count the total number of checked items
- Total Possible Score: 36
- 0–12 → High Risk
- 13–24 → Moderate Risk
- 25–36 → Controlled / IT-Ready



### Immediate Red Flags

- No documented support response times
- Backups not tested in last 90 days
- No HIPAA security controls documented
- Unsupported hardware in active use
- No monitoring or alerting configured
- No IT budget or roadmap documented



### Next Step

If your score indicates exposure, schedule a Dental IT Readiness Assessment.

[Dental IT Readiness Assessment](#) 