COMPLIANCE CHECKLIST · 2026

HIPAA Audit Checklist for Dental Practices

A fillable readiness checklist for HIPAA Security and Privacy Rules. Use during your annual review or before vendor selection.

How to use this checklist

This is a practical, dental-practice-oriented HIPAA checklist. It's not a substitute for a formal HIPAA risk assessment from a qualified consultant or attorney. Use it for self-audit, vendor evaluation, or as input to your formal annual review.

Three categories of HIPAA controls covered:

- Administrative safeguards — policies, training, risk assessment, access management.
- Physical safeguards — facility security, device controls, media handling.
- Technical safeguards — access controls, audit controls, encryption, transmission security.

Plus a Privacy Rule mini-checklist and a Business Associate review section.

Administrative safeguards

- [ ] Risk assessment completed in last 12 months
  Required by Security Rule. Updated when new tech or vendors added.
- [ ] Designated Privacy Officer and Security Officer
  Can be the same person in small practices.
- [ ] Workforce training completed annually
  All staff who touch PHI. Document attendance.
- [ ] Sanction policy for HIPAA violations
  Written, communicated, applied consistently.
- [ ] Information access management policy
  Role-based access to PHI; not everyone gets everything.
- [ ] Periodic access review (quarterly minimum)
  Audit who has access and remove unused accounts.
- [ ] Contingency / incident response plan
  Written plan, tested annually.
- [ ] Business Associate Agreements signed before vendor PHI access
  BAA on file for every vendor that touches PHI.

Physical safeguards

- [ ] Workstations facing patients are positioned to limit shoulder-surfing
- [ ] Workstation lockout / screensaver under 5 minutes idle
- [ ] Restricted physical access to server / network closet
  Locked. Logged when accessed.
- [ ] Visitor log and escort policy in clinical areas
- [ ] Disposal of paper PHI via locked shredder bin
  Or contracted shredding service with chain of custody.
- [ ] Inventory of all PHI-storing devices and media
  Workstations, laptops, tablets, USB drives, backup devices.
- [ ] Device encryption enabled (full-disk) on every workstation
  Required if any PHI on the device.
- [ ] Lost / stolen device protocol
  Remote wipe capability and incident workflow.

Technical safeguards

- [ ] Unique user ID for every workforce member with PHI access
  No shared logins.
- [ ] Automatic logoff configured
  <= 15 minutes idle.
- [ ] Encryption in transit for all PHI transmissions
  TLS 1.2+ for email, web, integrations.
- [ ] Encryption at rest for stored PHI
  Database encryption, full-disk encryption on devices.
- [ ] Audit logging of PHI access
  Who accessed what, when, from where.
- [ ] Multi-factor authentication on admin and PMS access
- [ ] Network firewall configured and reviewed quarterly
- [ ] Backup procedures with encrypted backups and tested restores
  Test restores at least annually.
- [ ] Email encryption for PHI transmissions to patients
  Or secure portal as alternative.
- [ ] Vendor risk review for any new SaaS handling PHI

Privacy Rule + Business Associate review

- [ ] Notice of Privacy Practices (NPP) posted and given to new patients
- [ ] Patient access request workflow defined
  Response within 30 days.
- [ ] Patient amendment request workflow defined
- [ ] Patient accounting-of-disclosures workflow defined
- [ ] Minimum necessary standard applied to PHI uses
- [ ] Authorization required for marketing uses of PHI
- [ ] BAA on file for: PMS vendor
- [ ] BAA on file for: Phone system / VoIP
- [ ] BAA on file for: Email provider (if PHI in email)
- [ ] BAA on file for: SMS / messaging
- [ ] BAA on file for: Cloud backup
- [ ] BAA on file for: AI receptionist or AI tools
- [ ] BAA on file for: Marketing / patient comms platform
- [ ] BAA on file for: Insurance verification clearinghouse

Result + next steps

Count completed boxes vs. total. Score below 80% means meaningful gaps to close before your annual HIPAA review or any audit.

BOXES COMPLETED (OF TOTAL)

_____ / ~40 items

DATE OF SELF-AUDIT

_____

AUDITOR / REVIEWER NAME

_____

TOP 3 GAPS TO CLOSE IN NEXT 30 DAYS

_____

Aria is HIPAA-aligned and signs a BAA same-day for new dental customers. If your practice is evaluating Aria as part of your AI vendor compliance review, we'll provide pre-prepared answers to your full HIPAA questionnaire on first call.

COMPLIANCE REVIEW QUESTIONS?

AriaDental.AI / demo

Email security@ariadental.ai or book a 30-minute compliance Q&A.