DENTAL IT

HIPAA Readiness Checklist

A practical 24-question self-assessment for dental practices

Purpose: Use this checklist to organize a readiness conversation around the HIPAA Security Rule. It is not a certification, legal opinion, or substitute for a complete risk analysis. A “yes” answer does not prove compliance, and a “no” answer identifies a topic that deserves follow-up.

How to score

For each question, mark **Yes**, **Partial**, **No**, or **Not sure**. Give yourself 2 points for Yes, 1 point for Partial, and 0 points for No/Not sure. Maximum score: 48.

Use the score as a prioritization aid only. HIPAA does not publish a universal checklist score that proves compliance.

Current-rule note (September 2026): HHS states that the current HIPAA Security Rule remains in effect. The rule requires reasonable and appropriate administrative, physical, and technical safeguards for ePHI. HHS continues to describe the rule as flexible, scalable, and technology neutral.

1. Governance and risk analysis

1. Have you documented where electronic protected health information (ePHI) is created, received, maintained, or transmitted across your practice?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

2. Have you completed and documented an accurate and thorough security risk analysis that reflects your current systems, vendors, locations, and workflows?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

3. Do you maintain a prioritized risk-management plan showing identified risks, owners, target actions, and completion status?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

4. Do you review security documentation when material technology, vendor, location, ownership, or workflow changes occur?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

2. Identity, access, and workforce controls

5. Does every workforce member use an individual account for systems that handle ePHI instead of shared administrator credentials?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

6. Are privileged and administrator rights limited to named people who need them and reviewed periodically?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

7. Is multi-factor authentication enabled where supported for remote access, email, cloud administration, and other high-risk accounts?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

8. Do you have documented onboarding, role-change, and offboarding steps that include timely access changes?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

3. Devices, systems, and technical safeguards

9. Do you maintain a current inventory of workstations, servers, laptops, network devices, cloud systems, and other technology that can store or reach ePHI?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

10. Are supported operating systems and security updates managed on devices that access ePHI?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

11. Are endpoint protection, secure remote access, firewall/network controls, and logging responsibilities clearly assigned and monitored?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

12. Have you evaluated encryption at rest and in transit for systems that store or transmit ePHI, documenting decisions where the current rule treats specifications as addressable?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

4. Backup, recovery, and continuity

13. Do you know exactly which clinical and business data is backed up, including practice-management databases and imaging repositories where applicable?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

14. Are backup administration and recovery copies protected from the same credentials or incidents that could affect production systems?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

15. Have you completed and documented a real restore test using representative systems or data rather than relying only on a successful backup status?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

16. Do you have documented procedures for data backup, disaster recovery, and emergency-mode operations during an outage or security incident?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

5. Vendors, business associates, and change control

17. Do you maintain an inventory of vendors that create, receive, maintain, or transmit PHI/ePHI on behalf of the practice?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

18. Have you confirmed appropriate business associate agreements are in place where required before sharing PHI/ePHI with a vendor?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

19. Do you control and review vendor remote-access methods, administrator accounts, and support pathways?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

20. Before major software, server, network, or cloud changes, do you verify backups, rollback options, vendor requirements, and responsibility boundaries?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

6. Training, incidents, and documentation

21. Do workforce members receive role-appropriate privacy/security training and security awareness education, with completion documented?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

22. Do staff know how to report suspicious email, lost devices, unauthorized access, malware, or other security events promptly?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

23. Do you have a documented incident-response process that identifies decision-makers, IT/vendor contacts, evidence-preservation steps, and escalation paths?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

24. Can you produce current policies, procedures, risk-analysis records, training records, incident documentation, and other required Security Rule documentation when needed?

[ ] Yes [ ] Partial [ ] No [ ] Not sure

Interpreting your result

40-48	Strong starting point. Validate evidence, test recovery, and address any Partial/No answers.
28-39	Several controls are in place, but important gaps or documentation weaknesses likely need an assigned remediation plan.
0-27	Prioritize a documented risk analysis and a focused remediation plan before treating the environment as ready.

Recommended next steps

1. Preserve evidence. Keep the risk analysis, risk-management plan, policies, training records, incident records, backup/restore evidence, and access-review documentation together so owners are clear.

2. Turn gaps into owners and dates. A readiness exercise is useful only if unresolved risks become tracked work with accountable owners and follow-up.

3. Use the HHS SRA Tool when appropriate. HHS and ONC provide a Security Risk Assessment Tool aimed at small and medium healthcare providers. It can help structure the process, but HHS does not present it as certification or a guarantee of compliance.

4. Get qualified help where needed. IT can help with technical safeguards and evidence. Legal/privacy questions, regulatory interpretations, and organization-specific compliance decisions may require qualified counsel or compliance professionals.

Primary references

HHS - Summary of the HIPAA Security Rule
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HHS - Guidance on Risk Analysis
https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

HHS/ONC - Security Risk Assessment Tool
https://healthit.gov/privacy-security/security-risk-assessment-tool/

Need a second set of eyes? Dental IT can help you inventory the technology environment, validate backup/recovery ownership, review technical safeguards, and turn findings into a practical remediation roadmap. Visit **itdental.tech/resources/hipaa-readiness-checklist/**.