

AGENTIC DENTAL OPERATIONS

Practice Attestation

Use of agentic systems with protected health information

Insert this signed original in the practice HIPAA compliance binder.

1. Covered entity

Legal name of practice	Covered entity legal name
Principal address	Street, city, state, ZIP
Effective date	Date this attestation takes effect

2. Purpose

This attestation records the practice’s decisions and continuing duties for Agentic Dental Operations: a three-zone arrangement in which the practice management system remains the system of record, a dedicated private-cloud environment running an agentic orchestration platform performs assigned work, and contracted AI model providers supply reasoning only under a Business Associate Agreement. Signing this document does *not*, by itself, make the practice HIPAA-compliant. It is evidence that the undersigned have reviewed the design, accepted the duties below, and authorized patient data to be used only after the stated conditions are met.

3. The practice affirms

A. System of record and minimum necessary

1. The practice management system and patient health information database stay where they are. Nothing in those systems is migrated, wholesale-replicated, or replaced as a condition of this arrangement.
2. Agents query practice systems through a defined interface of named operations. They are not issued a general database login, an admin console, or arbitrary query access.
3. Credentials for practice systems, messaging platforms, and AI providers are held in the private-cloud vault, scoped to specific agents and projects, injected only at the moment of use, and logged. They are not stored in scripts, tickets, configuration files, or agent notes.
4. Widening the interface, adding a credential, or granting an agent new access is a recorded change approved by a person before it takes effect.

B. Business associates and model use

5. Any vendor that creates, receives, maintains, or transmits protected health information on the practice’s behalf is treated as a business associate. No patient information is sent to that vendor until a Business Associate Agreement covering the intended use is fully executed.
6. For the model providers presently in scope: Anthropic (Claude) commercial API and Enterprise plans are used only after the BAA is executed by the organization’s owner, HIPAA coverage is activated on the account, and zero data retention is enabled. xAI (Grok) is used only after a signed BAA *and* use of the zero-data-retention API. Consumer subscriptions are not used for patient information. Features, endpoints, or plans outside the applicable BAA will not receive patient information.
7. Microsoft, as host of the dedicated Azure environment, and Standard Computer, as the party standing up and supporting the arrangement, are treated as business associates to the extent they handle protected health information, and are covered by a signed BAA before that handling begins.

C. Patient communications

8. A message about treatment the patient’s own dentist proposed is treated as a treatment communication. A message promoting products or services beyond that specific treatment — including whitening packages, membership plans, financing offers, or anything a third party paid to include — is treated as marketing.
9. Marketing to identified patients using their health information will not be sent without prior written patient authorization. Automated calls and texts are also governed by federal telemarketing law; the practice will not authorize those sends without the required documented consent.
10. No automated outbound message leaves the system unless the consent gate has verified, for that patient and that message type, that the required consent or authorization is on file and current, and that the patient carries no do-not-contact or deceased flag.
11. Agents personalize only within templates the practice Privacy Officer has approved. Novel outbound copy is not composed from scratch. Every message sent is retained with its template version, consent basis, and timestamp.

D. Officers, analysis, training, and records

12. The practice has designated, in writing, a Privacy Officer and a Security Official. Those designations are current as of the effective date and are recorded in the signature block below.
13. The practice maintains a current security risk analysis covering the whole practice, including this arrangement, and will update that analysis when the design or the use cases materially change.
14. The practice maintains the patient consent and authorization records the consent gate checks against, trains the workforce whose jobs are affected by this arrangement, and documents that training.
15. The practice retains this attestation, the related Business Associate Agreements, the Safeguards Summary, risk-analysis updates, template approvals, and training records for six years from the date of creation or last effective date, whichever is later.

E. Authorization to operate

16. Patient information will not be introduced into the agent environment until the validation stage described in the Risk Mitigation Summary has been completed and recorded: control checklist executed, restore tested, and safeguards documented.
17. Agents may not hire other agents, expand their own permissions, change budgets, or add credentials without a person's approval. A compliance reviewer sitting outside the delivery chain may block work that touches patient information or patient communication; a block escalates to a person and cannot be overridden by the lead agent.
18. The practice understands that written agent instructions (including SOUL.md and role documents) guide behavior and are not a substitute for the vault, scoped credentials, the consent gate, approval workflows, or the audit log.

4. What this document is not

This attestation is an internal record of the covered entity. It is not a Business Associate Agreement, not a substitute for the practice's security risk analysis, and not legal advice. Counsel for the practice should review the patient-communication standards, consent and authorization requirements, and telemarketing rules before the first outbound campaign.

5. Signatures

By signing, the covered entity's authorized official affirms the statements in Section 3 and authorizes the arrangement described in Section 2 as of the effective date above.

Authorized official <i>Binds the covered entity</i> Signature _____ Name / title _____ Date _____	Privacy Officer <i>Communications and consent</i> Signature _____ Name / title _____ Date _____	Security Official <i>Technical and risk analysis</i> Signature _____ Name / title _____ Date _____
---	---	--