

A GUIDE FOR DENTAL & HEALTHCARE PRACTICES

AI Is Already In Your Practice. Nobody Approved It.

A straight answer on keeping patient data out of AI tools you don't control,
and a Copilot rollout that actually holds up under a HIPAA audit.

THE AI EXPOSURE SCALE

YOUR FIRST 90 DAYS

WHAT ACTUALLY COUNTS
AS COMPLIANT

2026

Let's Not Pretend This Isn't Happening

Your office manager is asking ChatGPT to draft the recall letter for patients who haven't been in since last year. Your front desk is pasting insurance correspondence into a free AI tool to get the appeal written faster. Someone on your billing team is summarizing a patient's account history so they don't have to read the whole thing before the call.

None of them cleared it with you first. Most of them don't think there's anything to clear.

“

Nearly 1 in 5 healthcare workers and administrators admit to personally using an AI tool their employer never approved. More than 40 percent say they know a coworker who has.

WOLTERS KLUWER HEALTH, [SHADOW AI: A HIDDEN RISK TO HEALTHCARE](#), JAN. 2026

You're not reading this because you think AI is dangerous. You're reading it because you already suspect there's patient information moving through tools you've never reviewed, and you don't have a clean answer for what happens next.

This guide is that answer. Not a lecture on AI ethics. A plan you can actually run in a practice that's already busy enough.

What Your Team Is Probably Already Doing

You don't have an AI policy yet. That doesn't mean AI isn't already in the building. Here's what we typically find once we start asking:

- Drafting patient letters, recall reminders, and review responses in seconds instead of ten minutes
- Pasting chart notes or referral letters into a free tool to clean them up or summarize them
- Asking AI to explain an insurance denial or draft the appeal language
- Writing job postings, onboarding checklists, and internal memos
- Summarizing long email threads before anyone reads the original

None of this makes your staff careless. They're doing what anyone does when a tool makes a tedious task faster. The problem isn't intent. It's that nobody told them where the line is, because nobody drew one.

Not staff ignoring a policy.

Staff inventing their own, because nobody wrote one.

Not an AI ban.

An AI plan your practice actually controls.

Not scared of AI.

Scared of finding out the hard way.

Why This Is Worth Twenty Minutes of Your Time

Patient Data Leaves the Building

The note that got pasted into a free AI tool now lives on a server you don't control, inside a company you have no agreement with. That's protected health information outside your practice's custody.

Your BAA Might Not Cover It

Your practice has business associate agreements for the vendors you know about. A free AI tool isn't one of them, and it never signed anything promising to protect what got pasted in.

Someone Answers to OCR

If this ever surfaces in a complaint or a breach investigation, the Office for Civil Rights isn't going to ask which AI tool did it. They're going to ask what your practice's policy was.

Your Patients Notice

Patients trust you with things they don't tell anyone else. Finding out their information passed through a tool nobody vetted doesn't just risk a fine. It risks the relationship.

Some practices are getting real time savings out of AI. Others are taking on the exposure without any of the control. That's not a trade worth making by accident.

Start With What You're Already Paying For

Before you evaluate another AI vendor, look at what's already sitting inside your Microsoft 365 subscription. Your email is in Exchange. Your files are in SharePoint and OneDrive. Your team already meets in Teams. Copilot doesn't ask you to move any of that. It works inside the environment you already pay for, and in most cases already have us managing.

That matters more than it sounds like it should. It's not a new platform to vet, a new BAA to chase down, or one more login for your team to forget. It's the same front door, with AI turned on behind it.

One thing worth being precise about: Copilot works with what lives in Microsoft 365. It doesn't reach into Oryx, Dentrix, Eaglesoft, or whatever practice management system holds your actual clinical records, unless that data has been synced or exported into your Microsoft environment. That's a feature, not a gap. It keeps the blast radius smaller while you get the rest in order.

“

43.3 percent of U.S. dentists already use AI for at least one task in their practice, and another 26.4 percent plan to adopt it soon. Adoption isn't the open question anymore. Governance is.

AMERICAN DENTAL ASSOCIATION HEALTH POLICY INSTITUTE, 2026

The AI in healthcare market is projected to grow from \$36.7 billion in 2026 to nearly \$195 billion by 2031. Practices that put governance in place now won't be scrambling to catch up later. (MarketsandMarkets, 2026)

Why Microsoft 365 Makes Sense for a HIPAA Practice

Your Data Doesn't Leave the Tenant

Copilot runs inside your Microsoft 365 environment. It isn't training a public model on your patients' information, and it isn't shipping data to a company you've never heard of.

Your Permissions Do the Enforcing

Copilot only surfaces what a given user can already see. If someone can pull up a file they shouldn't have access to, that's a permissions problem Copilot just made visible.

Your Security Stack Already Covers It

It lives alongside Defender, Entra ID, and whatever compliance tooling is already protecting your tenant. Nothing new to bolt on.

Your Team Already Knows the Tools

It shows up inside Word, Outlook, and Teams. No separate app, no separate login, no training program that starts from zero.

What actually counts as compliant

Copilot being available on a HIPAA-eligible plan doesn't make your practice compliant by default. Your practice has to accept Microsoft's Business Associate Agreement in the admin center, and Copilot has to be running under a license that falls inside Microsoft's Enterprise Data Protection commitments, meaning prompts, responses, and the Microsoft Graph data behind them aren't used to train Microsoft's models. One nuance worth knowing: that protection covers what's inside your tenant, not open web results Copilot sometimes pulls into an answer. Anything that reaches the public web gets treated like information from any other public source, not something HIPAA automatically covers.

The AI Exposure Scale

This is the lens we use to evaluate where a practice actually stands, built around how AI risk plays out specifically in a HIPAA environment. Most practices land at Level 1 before anyone's looked closely. Most don't realize it until someone asks.

1

Untracked AI SEVERE

Staff are already using AI tools. Nobody in the practice knows which ones, how often, or what's being typed into them.

2

Written, Not Read HIGH

A policy exists somewhere, probably in a binder or a shared drive nobody opens. No training happened. No one is enforcing it.

3

Controlled Pilot MODERATE

A small group, clear rules, no PHI going anywhere ungoverned, results actually tracked. This is where you want to be before you go further.

4

Managed Rollout LOW

Wider access, logging turned on, permissions audited on a schedule. AI is something your practice manages, not something you're hoping nobody notices.

5

Compliant by Design CONTROLLED

Copilot, automation, and whatever comes next, all running inside a BAA-covered, access-controlled environment. You expanded from a position of control, not cleanup.

What Has to Be True Before You Scale

Turning on Copilot before your environment is ready just puts a spotlight on problems that were already there. Before you scale past a small pilot, work through these:

Identity & Access

- ☐ Is everyone logging in with their own licensed account? Nobody should be sharing a login or using a personal email for practice business.
- ☐ Who still has access from the front desk person who left eight months ago?
- ☐ Do you actually know how many people have the password to that one shared inbox everyone uses?

SharePoint & Teams

- ☐ Any folder set to "Everyone" that really shouldn't be? Find it.
- ☐ Old case files or project folders that outlived the reason anyone needed them? Archive them or lock them down.

Data Classification

- ☐ Is anything actually labeled as containing PHI, or is that just something everyone assumes they'll recognize when they see it?
- ☐ If your practice can't say what's sensitive, Copilot can't either.

Acceptable Use Policy

- ☐ You need one. It doesn't need to be forty pages. It needs to exist, get communicated, and actually get enforced.
- ☐ Review it every quarter. What's true about AI today won't be true in six months.

This isn't about making AI harder to use. It's about making sure the AI your team is already using doesn't outrun what your practice can actually stand behind.

Where AI Goes Next

Once governance is handled, the upside is real. Everything below assumes you've already done the work on the pages before this one. Skip that work and you're just adding new surface area to the same risk.

- Insurance verification and eligibility checks handled automatically, with a human confirming before anything goes to the patient
- Recall and reminder campaigns drafted and personalized in bulk instead of one at a time
- Billing follow-up and appeal letters drafted from account history, reviewed before they go out
- Scheduling and front-desk workflows that flag conflicts before they become a missed appointment

None of this replaces clinical judgment, and none of it should touch a chart without a person reviewing it first. It just means the paperwork stops eating the hours your team should be spending with patients.

Your First 90 Days

Here's the practical plan for getting AI under control while still getting value out of it.

DAYS 1 TO 30

Find Out What's Actually Happening

- ☐ Ask your staff directly what AI tools they're using and how often. Don't punish honest answers, you need them.
- ☐ Audit your Microsoft 365 environment: permissions, sharing settings, shared mailboxes, all of it.
- ☐ Identify where PHI actually lives across email, files, and shared drives.
- ☐ Draft a basic acceptable use policy. It doesn't need to be perfect. It needs to exist.
- ☐ Get a HIPAA and AI readiness assessment from a partner who already knows Microsoft 365.

DAYS 31 TO 60

Get the Environment Ready

- ☐ Fix the permissions problems the audit surfaced.
- ☐ Finalize the policy and get sign-off from whoever runs the practice.
- ☐ Confirm the Microsoft BAA is signed and Copilot is enabled on an eligible license.
- ☐ Pick a pilot group of five to eight people across different roles: front desk, billing, clinical support.

DAYS 61 TO 90

Learn, Expand, Report

- ☐ Ask the pilot group what worked and what didn't.
- ☐ Refine the policy based on what you actually learned, not what you assumed going in.
- ☐ Expand access to the rest of the practice under the same rules.
- ☐ Report to leadership or ownership. Show the time saved and the risk that's now under control.
- ☐ Make the permissions review a recurring habit, not a one-time cleanup.

Where BLS IT Comes In

We've spent years inside Microsoft 365 environments for dental and healthcare practices. We know HIPAA, we know how a front desk actually works, and we're not going to hand you a forty-page policy nobody will read.

HIPAA & AI Readiness Assessment

We find out what's already exposed before you find out the hard way.

Microsoft 365 Security Review

Permissions, sharing, shared mailboxes. The works.

Acceptable Use Policy

Written in plain English, short enough that people actually read it.

Copilot Pilot Design & Launch

We handle the BAA confirmation, the licensing, and the rollout.

Ongoing Governance

This isn't a one-time project, and we don't treat it like one.

Here's the Deal

You can keep letting this happen without a plan. Your team will keep finding faster ways to get through the day, and the exposure will keep growing quietly until it isn't quiet anymore.

Or you can spend 90 days getting it under control. That's not a lot of time for something this important.

We'll tell you exactly where you stand, what's exposed, and what to fix first. Then we'll help you turn Copilot on the right way, so the next AI tool your team wants to use is a decision you get to make on purpose instead of something you find out about later.

Schedule a HIPAA and AI readiness assessment with BLS IT, and find out where your practice actually stands.

SOURCES

1. Wolters Kluwer Health, "Shadow AI: A Hidden Risk to Healthcare," January 2026
2. American Dental Association Health Policy Institute, "Dentists' AI Usage and Attitudes," 2026
3. MarketsandMarkets, "Artificial Intelligence in Healthcare Market," 2026
4. Microsoft Learn, "Enterprise data protection in Microsoft Copilot and Microsoft Copilot Chat," 2026

About BLS IT

BLS IT is a managed IT provider based in Salem, Massachusetts, built around flat-rate, all-inclusive support for healthcare and dental practices across the North Shore, Greater Boston, and into New Hampshire, Vermont, and Maine. We focus on HIPAA compliance, Microsoft 365, and the security stack that has to sit underneath both, so practices can adopt tools like Copilot without gambling on patient trust to do it.