SIMON SAYS SYSTEMS

LOCAL DENTAL IT & HIPAA SPECIALISTS
SW RIVERSIDE COUNTY, CA

HIPAA COMPLIANCE CHEAT SHEET · DENTAL

The Dental Practice Owner's HIPAA Cheat Sheet

Everything a 1–10 provider practice in SW Riverside County actually has to do — and what it costs you if you don't. In plain English, on one page.

You went to dental school, not law school. Here's the whole compliance picture without the 200-page binder — so you know the right questions to ask before an auditor or a breach decides it for you.

1 The Mandate — What Law Applies

Two governments regulate your patient data. Both can write you a check you don't want to cash.

- **HIPAA (federal):** Privacy Rule (who can see PHI), Security Rule (how you protect the electronic version — charts, imaging, e-claims), Breach Notification Rule. Enforced by the **HHS Office for Civil Rights (OCR)**.
- **CMIA — California's layer** (Confidentiality of Medical Information Act, Civil Code §56 et seq.): stricter than HIPAA and stacks on top. Its sharpest edge: **patients can sue you directly** — no government investigation required. Enforced by the **CA Attorney General**, DAs/city attorneys, and private lawsuits.

Plain English: a single CA breach is a **two-front problem** — a federal regulator *and* a courtroom full of patients' attorneys.

2 What Compliance Requires — The Must-Do List

- **Security Risk Analysis (SRA)** — written, honest, updated **annually** + on any change. *The #1 thing OCR fines practices for not having.* Not a one-time PDF.
- **Three safeguard layers:** Technical (encryption, unique logins, auto-logoff, audit logs — **no shared front-desk password**); Administrative (named security officer, policies, incident plan); Physical (locked server, screens off the lobby, wiped devices).
- **A signed BAA with every vendor that touches PHI** — IT, cloud backup, imaging host, email. **A missing required BAA is itself a HIPAA violation** — it can be cited even if no patient data was ever exposed.
- **Workforce training** — every hire, with proof kept. **Breach procedure** — patients + HHS within **60 days**; CA adds AG notice for breaches over 500 residents.
- **Encryption & audit logging on by default.** Encryption is your **safe harbor** — a lost-but-encrypted laptop usually isn't a reportable breach.

The SSS throughline: most of this list is the **technical layer we own for you.** You run the practice; we handle the safeguards and hand you the documentation when the auditor asks.

The Penalties — What It Costs to Get This Wrong

Federal HIPAA civil penalties (OCR), per violation.
One missing safeguard across thousands of records can count as thousands of violations.

TIER	WHAT HAPPENED	PER VIOLATION	ANNUAL CAP
1 — No knowledge	Didn't know, couldn't reasonably have known	**$145 – $73,011**	up to $2,190,294
2 — Reasonable cause	Knew or should have, not willful neglect	**$1,461 – $73,011**	up to $2,190,294
3 — Willful neglect, fixed in 30 days	Ignored, then corrected	**$14,602 – $73,011**	up to $2,190,294
4 — Willful neglect, never fixed	Ignored, didn't correct	**$73,011 – $2,190,294**	**$2,190,294**

Effective Jan 28, 2026. OCR currently applies lower annual caps to Tiers 1–3 by enforcement discretion — a policy choice it can reverse, not law.

CRIMINAL (REFERRED TO THE U.S. DEPARTMENT OF JUSTICE) — STATUTORY MAXIMUMS

Up to **$50,000 + 1 yr** (knowingly obtaining/disclosing PHI); **$100,000 + 5 yrs** (false pretenses); **$250,000 + 10 yrs** (intent to sell/transfer PHI for gain). Reserved for knowing misconduct, not paperwork gaps.

CALIFORNIA STACKS CMIA ON TOP (CIVIL CODE §56 ET SEQ.)

Under §56.36, patients can sue you directly for **$1,000 nominal damages per patient** — no proof of actual harm needed, though a **2026 CA Supreme Court ruling** now requires showing a *significant risk* the data was accessed — plus actual damages and fees. Civil fines **$2,500** / **$25,000** / **$250,000** per violation.

What an OCR Investigation Looks Like

Usually triggered by a breach report, patient complaint, or OCR's **Risk Analysis Initiative** (16+ settlements in 2025). First words: *"show us your documentation."* No current SRA = they presume non-compliance. Settlements run **~$100K into the millions**, almost always with a multi-year **Corrective Action Plan**.

Honest bottom line: for a small practice, even a low-six-figure outcome + a Corrective Action Plan defines a year. Don't leave the technical safeguards to chance.

WAIT — BUT WHAT ABOUT...

"My IT guy handles this."
Ask him: *"When was our last documented Security Risk Analysis, and can I see it?"* General IT keeps computers running; HIPAA technical safeguards — encryption, access logs, the signed BAA, the SRA on file — are a different job, and the one OCR asks about first. No document = you don't have it.

"We're too small to be a target."
Enforcement isn't about size; it's about whether your safeguards are documented when something goes wrong. OCR has fined solo and small dental practices **tens of thousands of dollars over a single patient's records-access complaint** (e.g., a 2024 dental settlement of $70,000). (We're a small local shop too — that's the point; we fit practices your size.)

Not sure where YOUR practice actually stands? Find out for free.

We'll do a **free HIPAA technical security review** of your practice — a local specialist looks at your actual setup (network, backup, EDR, email, vendor BAAs, and whether you have a current Security Risk Analysis on file) and gives you a **plain-English findings list:** where your technical safeguards are solid and where the gaps are. No sales pitch, no jargon, no obligation. **We never ask for patient information** on the call.

Book your free security review →

simonsayssystems.com/dental-review · or call/text Craig direct: (951) 717-3576

Local to Menifee. Remote-first, on-site across Temecula, Murrieta, Wildomar, Lake Elsinore & Sun City.