HIPAA COMPLIANCE CHEAT SHEET · MEDICAL

The Private Practice's HIPAA Cheat Sheet — Medical Edition

Everything a 1–10 provider medical 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 med school, not law school — and "the EHR vendor handles compliance" is the assumption that gets practices fined. Here's the whole picture without the 200-page binder, so you (or your practice manager) 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 — your EHR/EMR, e-prescribing, lab/imaging results, 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 patient lawsuits.

Plain English: a single CA breach is a **two-front problem** — a federal regulator *and* a courtroom full of patients' attorneys. A medical practice moves more PHI through more systems — EHR, portal, clearinghouse, e-prescribing, labs — than almost any small business in town, which means more places for it to leak.

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* — and not something your EHR vendor does for you. Not a one-time PDF.
- **EHR access logging & unique logins — actually on and reviewed.** Each provider/staffer gets their own credentials; the system logs who opened which chart. **No shared "nurses' station" password.**
- **Patient-portal security** — MFA, session timeouts, access controls on the portal patients log into. It's an internet-facing door into your PHI.
- **A signed BAA with every vendor that touches PHI** — EHR/EMR host, e-prescribing, the **clearinghouse**, lab/imaging interfaces, cloud backup, IT, email. **A missing required BAA is itself a HIPAA violation** — medical has the longest vendor chain of any small office, the most common gap we find.
- **The three safeguard layers + breach procedure:** Technical (encryption, unique logins, auto-logoff, audit logs); Administrative (named security officer, policies, incident plan, training with proof); Physical (locked server, screens off the waiting room, wiped devices). Breach: patients + HHS within **60 days**; CA adds AG notice for breaches over 500 residents. Encryption is your **safe harbor**.

The SSS throughline: most of this is the **technical layer we own for you** — access logs, encryption, portal and clearinghouse vendor BAAs, the SRA on file. 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

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. More systems, more PHI, more surface area to get this wrong. Don't leave the technical safeguards to chance.

WAIT — BUT WHAT ABOUT...

"My IT guy / EHR vendor handles this."

Maybe parts of it. Ask: *"When was our last documented Security Risk Analysis, and can I see it?"* Your EHR vendor secures *their* platform and signs *their* BAA — they don't run your network, review your access logs, confirm your clearinghouse and e-prescribing BAAs, or keep your SRA. 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 settled over a **single patient's records-access complaint** — e.g., OCR's **$112,500** Right-of-Access settlement in December 2025 (its 54th such action) — and in an earlier action, **$15,000** from a small provider that ignored OCR's technical assistance and still wouldn't hand over records. (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, EHR access logging, patient-portal security, 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/medical-review · or call/text Craig direct: (951) 717-3576

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