HIPAA Readiness Self-Check

A 5-minute gap analysis for small healthcare practices

Answer each question honestly. Check the box next to every statement that is currently true at your practice. At the end, count your checked boxes — the scoring guide on page 2 tells you what your number means and what to do next.

1. Privacy Rule & Patient Rights

- ☐ **1.** We have a current Notice of Privacy Practices (NPP) reviewed in the past 12 months and made available where patients can find it.
- ☐ **2.** We have a written process for responding to patient requests for access, amendment, and accounting of disclosures — within the HIPAA-required timelines.
- ☐ **3.** We obtain written authorization before any use or disclosure of PHI beyond treatment, payment, and operations (e.g., marketing, research, psychotherapy notes).
- ☐ **4.** We have a designated Privacy Officer named in writing — even if that person is the practice owner.

2. Security Rule & Technical Safeguards

- ☐ **5.** We have completed a written HIPAA Security Risk Analysis within the past 12–18 months, with a documented remediation plan.
- ☐ **6.** Every device used to access, store, or transmit PHI (laptops, phones, tablets) is encrypted and requires a password or biometric login.
- ☐ **7.** Every workforce member who accesses the EHR has a unique login (no shared accounts), and we remove access within 24 hours of departure.
- ☐ **8.** We maintain a written information-security policy reviewed and acknowledged by workforce within the past year.

3. Business Associate Agreements (BAAs)

- ☐ **9.** We maintain a current inventory of every vendor that touches PHI — EHR, email, scheduling, billing, AI scribes, cloud storage, messaging, transcription.
- ☐ **10.** We have a signed, current BAA on file for every vendor on that list.
- ☐ **11.** Each BAA includes current HIPAA language, including breach-notification timelines and subcontractor flow-down obligations.
- ☐ **12.** We review vendor BAAs at least annually and whenever the vendor relationship changes (new services, pricing tier, ownership change).

4. Breach Response Readiness

- ☐ **13.** We have a written Breach Response Plan stored where we can reach it quickly under pressure (not just on the compromised system).
- ☐ **14.** We know the HHS OCR notification timelines (60 days for breaches affecting 500+ individuals; annually in aggregate for smaller breaches) and our state's breach-notification deadline.
- ☐ **15.** We maintain an incident log documenting every potential incident, our breach-risk analysis, and the outcome — whether or not notification was triggered.
- ☐ **16.** We have identified our breach-response team in advance: counsel, cyber-insurance carrier, forensic firm, and notification vendor contacts are documented.

5. Policies, Training & State Overlay

- ☐ **17.** We have a documented, customized set of HIPAA policies (Privacy, Security, Breach Notification) — not just unmodified templates pulled from the internet.
- ☐ **18.** Every workforce member completes HIPAA training at hire and at least annually, with a signed attestation we can produce in an audit.
- ☐ **19.** We know what our state requires on top of HIPAA (e.g., mental-health records statutes, stricter telehealth or minor-consent rules, state breach-notification timelines).
- ☐ **20.** If we deliver telehealth, we have reviewed: informed-consent scripts, platform BAAs, cross-state licensing implications, and state telehealth-specific requirements.

Your Score — Count Your Checked Boxes

17–20	Strong baseline. Tighten the remaining gaps and set a calendar for annual review.
12–16	Functional, with several meaningful gaps. A focused audit will close them quickly.
7–11	Substantial exposure. A HIPAA Readiness Audit is the right next step — before anything goes wrong.
0–6	High risk. Book a call this week. The practices that wait are the ones that pay the most later.

What to do next

Whatever your score — even a strong one — a free 15-minute readiness call gives you a straight read on which gap is worth fixing first. No pitch. No pressure.

Book a Free 15-Minute Readiness Call

calendly.com/dadybentleyz/intro-privacy-meeting

Or email: Ferdinand.n@lionsprivacygroup.com