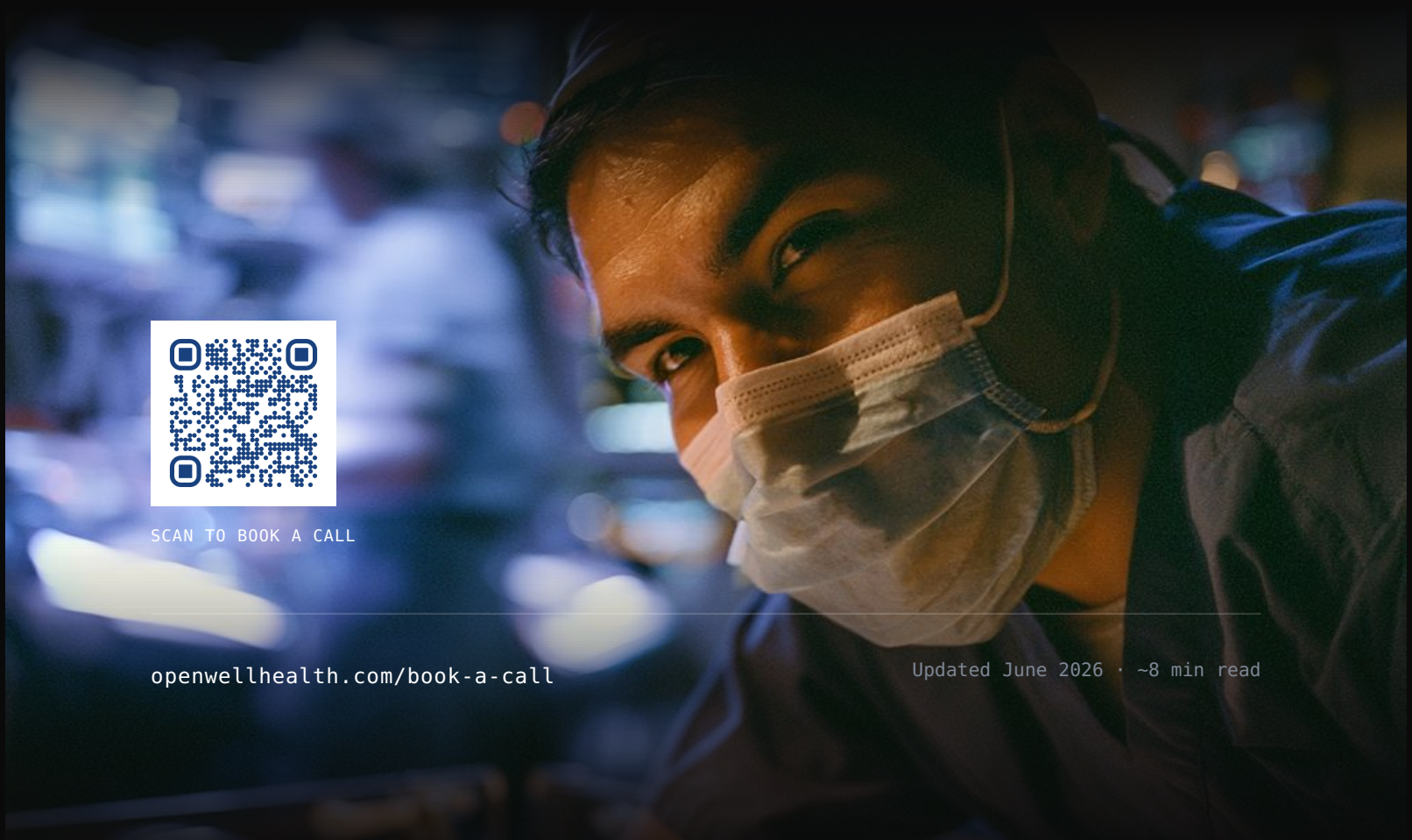
OPENWELL · RESOURCE BRIEF

HIPAA & COMPLIANCE

HIPAA Compliance for a New Clinic: What You Actually Need on Day One

Day-one HIPAA for a new clinic: risk analysis, BAAs with every PHI vendor, core safeguards, a privacy notice, training, and a breach plan — no enterprise bloat.



SCAN TO BOOK A CALL

openwellhealth.com/book-a-call

Updated June 2026 · ~8 min read

HIPAA & COMPLIANCE

A new clinic is HIPAA-compliant on day one with seven things: a documented security risk analysis, a signed Business Associate Agreement (BAA) with every vendor that touches patient data, core technical safeguards (encryption, access controls, MFA, audit logs), a Notice of Privacy Practices, patient consent forms, documented workforce training, and a written breach protocol. **The single highest-leverage rule is the vendor one: no BAA, no PHI — if a vendor won't sign, that vendor does not handle your patient data.** None of this requires enterprise compliance software or a consultant on retainer.

What HIPAA actually requires of a small practice

HIPAA scales with you. The rule sets — Privacy, Security, Breach Notification — apply to a solo cash-pay clinic just as they do to a hospital system, but the Security Rule explicitly expects safeguards "reasonable and appropriate" to your size and complexity. A solo practice doesn't need a compliance department; it needs a defined, documented, working set of safeguards. The trap for new clinics isn't doing too little of the exotic stuff — it's skipping the boring required stuff: the risk analysis, the BAAs, and the documentation.

One scoping note: HIPAA applies to you as a covered provider regardless of payment model. A cash-pay practice with no insurance billing still holds PHI and still complies.

The risk analysis is not optional, and "small" is not a defense.

FROM THE BRIEF

The day-one stack, in order

1. Run the security risk analysis (required, and first)

The risk analysis is the foundational, explicitly required step: inventory where PHI lives (EHR, messaging, email, phone, laptop, lab portals), identify threats and gaps, and document what you'll do about them. For a new solo practice this is a focused working session, not a six-month project — but it must be written down. "We did it in our heads" is the most common audit failure mode. Revisit it annually and when your systems change.

2. Sign a BAA with every vendor that touches PHI

A Business Associate Agreement is the contract that obligates a vendor handling PHI on your behalf — EHR, membership billing, secure messaging, email provider, cloud storage, transcription, answering service, hosting — to protect it. The operating rule, verbatim from how disciplined platforms run it: **no BAA, no PHI.** A vendor without a BAA doesn't ship into your stack.

Make the BAA question the *first* filter in every software decision, not the last: it instantly disqualifies consumer tools (standard Gmail, regular SMS, consumer video apps) and saves you from discovering at launch that a tool you've built around won't sign. That late discovery is one of the classic launch mistakes. The Biggest Mistakes Doctors Make When Starting a Practice

3. Put the core technical safeguards in place

For a small practice, four controls cover the bulk of the Security Rule's technical expectations:

EXHIBIT

SAFEGUARD	DAY-ONE MINIMUM
Encryption	PHI encrypted in transit and at rest (AES-256 is the standard); full-disk encryption on any laptop or phone touching PHI
Access control	Role-based access — each person sees only what their role requires; unique logins, never shared accounts
Multi-factor authentication	MFA on every system that touches PHI, no exceptions, including email
Audit logs	Systems that log who accessed what, with logs retained; keep HIPAA documentation on the order of six-plus years

If you choose a HIPAA-compliant EHR/platform that signs a BAA, most of this arrives built in — encryption, RBAC, MFA, audit logging are platform properties, not projects. Your remaining exposure is the edges: your email, your phone, your laptop, your habits.

4. Publish your Notice of Privacy Practices

The NPP tells patients how their information is used and disclosed and what their rights are. Post it in the practice and on the website, provide it at first encounter, and document acknowledgment. Templates are widely available; tailor one to your practice rather than drafting from scratch.

5. Prepare patient consent and intake forms

Consent for treatment, authorization forms for disclosures beyond treatment/payment/operations, and — for membership practices — the financial-responsibility/membership agreement. Build these into digital intake from day one so signed copies are stored, not scattered.

6. Train yourself and anyone who works with you — and document it

Workforce training is required, at hire and at least annually, and "workforce" includes you, a part-time MA, a virtual assistant, and anyone else touching PHI. For a small practice this is an hour of structured training plus a signed attestation. The documentation is the point: undocumented training doesn't exist, as far as an auditor is concerned.

Adopt two working habits that do more than any policy binder: **minimum necessary** (share only the PHI a task requires — internally, reference patients by ID rather than name where possible) and **clean**

channels (patient communication happens in the secure platform, not personal text or standard email).

7. Write the breach protocol before you need it

A one-page written plan: how you identify and contain an incident, who assesses whether PHI was compromised, how you document it, and whom you notify. HIPAA's Breach Notification Rule sets specific duties — notifying affected individuals, notifying HHS, and notifying media for large breaches — on defined timelines. Most small-practice incidents are mundane: a misdirected email, a lost phone. The difference between a mundane incident and a reportable disaster is often whether the device was encrypted and whether you followed a written process. That's why steps 3 and 7 are connected.

What this looks like as a checklist

1. Security risk analysis completed and documented; review date on the calendar.
2. PHI vendor inventory written; BAA signed with every vendor on it.
3. Encryption, RBAC, MFA, and audit logging confirmed on every PHI system; devices encrypted.
4. Notice of Privacy Practices posted, provided, acknowledgment captured.
5. Consent, authorization, and financial-responsibility forms in digital intake.
6. Training completed and documented for everyone, including you; annual recurrence scheduled.
7. Written breach protocol filed where you can find it on a bad day.
8. A named privacy/security officer — in a solo practice, that's you, in writing.

What people get wrong

The pattern across new clinics is treating HIPAA as an afterthought — something to "get to" after the EHR, the website, and the first patients. It runs backward: compliance decisions are *vendor* decisions, and vendor decisions happen early. The practice that asks "will you sign a BAA?" first never has to migrate off a non-compliant tool later; the practice that asks last rebuilds its stack in month two. The second misconception is the opposite failure: assuming compliance requires enterprise machinery — GRC software, a hired compliance officer, five-figure consultants. For a solo or small clinic, it requires the seven items above, documented, on systems that are compliant by construction. Buying bloat

doesn't just waste money; it usually substitutes for the simple required things, which still don't get done.

Reality check

- **The risk analysis is not optional, and "small" is not a defense.** It's the explicitly required step regulators look for first, and small practices are not exempt from enforcement. Skipping it is the cheapest fine-print mistake in the launch.
- **Your biggest real-world risks are boring.** Unencrypted laptops, personal texting with patients, shared logins, and a vendor nobody got a BAA from. The exotic threats make headlines; the boring ones make breach reports.
- **Compliance is a practice, not a binder.** The documents matter, but the daily habits — clean channels, minimum necessary, MFA — are what actually protect patients. A perfect policy set with sloppy habits fails both ways.
- **Platforms remove most, not all, of the burden.** A HIPAA-compliant platform with a BAA handles the technical safeguards; the risk analysis, training, NPP, and your own devices and habits remain yours.
- **State law stacks on top.** Several states add privacy and medical-record requirements beyond HIPAA. This varies by state — have your forms and retention practices checked by a healthcare attorney licensed in yours.

This is general information, not legal or compliance advice; confirm requirements for your specific situation.

Frequently asked

What does a new clinic need to be HIPAA compliant on day one?

Seven things: a documented security risk analysis, BAAs with every PHI vendor, technical safeguards (encryption, role-based access, MFA, audit logs), a Notice of Privacy Practices, patient consent forms, documented training, and a written breach protocol. A solo practice can stand all of this up in weeks, especially on an already-compliant platform.

Does HIPAA apply to a cash-pay practice that doesn't bill insurance?

Operate as if yes. You hold PHI either way, state privacy laws apply regardless, and ordinary practice realities (e-prescribing, labs) pull you into scope. Full compliance is the only sensible operating assumption.

What is a BAA and which vendors need one?

A Business Associate Agreement is the contract requiring a vendor that creates, receives, stores, or transmits PHI on your behalf to safeguard it — EHR, billing, messaging, email, cloud storage, answering services, transcription. The rule: no BAA, no PHI. A vendor that won't sign doesn't touch patient data.

Do I need to hire a HIPAA compliance officer or consultant?

No. You must designate someone responsible for privacy/security — in a solo practice, yourself, in writing — and complete the required elements. Consultants can help with the risk analysis if you want a second set of eyes, but enterprise compliance tooling is not a day-one requirement for a small clinic.

Can I text or email my patients?

Not on standard SMS or consumer email — those channels typically lack encryption and BAAs. Use the secure messaging built into a HIPAA-compliant platform, or a messaging vendor that signs a BAA. Patient communication channels are the most common everyday compliance leak in small practices.

How often do I need HIPAA training?

At hire and at least annually for everyone who touches PHI — including you — with documentation each time. Undocumented training counts for nothing in an audit.

HOW OPENWELL CAN HELP

Done-for-you, end to end.

Openwell builds this compliance stack — risk analysis support, BAAs across the vendor chain, encryption and access controls, consent architecture, and the documentation — into the practice launch itself, so HIPAA is a configuration step rather than a months-long side project.

Book a call → openwellhealth.com/book-a-call

SCAN TO BOOK

RELATED OPENWELL BRIEFS

- How to Start Your Own Medical Practice From Scratch: The Complete Sequence
- The Complete Checklist for Opening a New Medical Practice
- What Software You Need to Run an Independent Medical Practice
- Best EMR for a Small Independent Practice (and How to Choose)