

HIPAA Compliance Self-Assessment for Small Practices

Score your practice across nine domains and surface your highest-risk gaps in about 20 minutes

This is a self-scored worksheet for a solo or 1-5 provider practice. Work through each domain, check the items you can honestly answer yes to, and leave the rest unchecked -- the unchecked boxes become your remediation list. If you only fix one thing, fix the Security Risk Analysis.

1. Security Risk Analysis and Risk Management

The single most common finding in a small-practice audit or breach investigation is a missing, never-done, or years-old Security Risk Analysis (SRA). A current SRA is generally required under 45 CFR 164.308, and it is the document that every other safeguard hangs off of. 'We bought an EHR that says it is HIPAA compliant' is not a risk analysis -- the analysis is about your whole environment, not one vendor's software.

Score each item yes only if you can point to a dated document or record, not a memory of intending to do it.

- ☐ A written Security Risk Analysis exists and covers all systems that create, receive, maintain, or transmit PHI -- not just the EHR
- ☐ The SRA was completed or updated within the last 12 months, or after the last major change (new software, new location, new vendor)
- ☐ Identified risks were ranked by likelihood and impact, not just listed
- ☐ A written risk management plan assigns each high risk an owner and a target fix date
- ☐ You can produce the dated SRA document today if asked

An SRA is a periodic, ongoing requirement -- a one-time analysis from three years ago does not count as current.

2. Policies and Documentation

Written policies are generally required, and 'we all just know how we do things' is not a defense. The test is whether a new hire could read your policies and follow them, and whether you can show the documents were reviewed recently.

- ☐ Written Privacy Rule and Security Rule policies exist and are specific to this practice, not a generic unedited template
- ☐ Policies have a review date within the last 12-24 months and a named person responsible
- ☐ A current Notice of Privacy Practices (NPP) is in use and posted
- ☐ Documentation (SRA, training logs, BAAs, incident records) is retained for at least 6 years
- ☐ Someone is formally designated as the Privacy Officer and Security Officer (can be the same person in a small practice)

3. Workforce Training and Sanctions

Most small-practice breaches start with a person, not a hacker -- a misdirected fax, a clicked phishing link, a chart left open. Training is generally required, and it has to be documented and repeated, not done once at hire and forgotten.

- ☐ Every workforce member completed HIPAA training, with a dated record (sign-in or completion log) for each person
- ☐ Training is repeated at least annually and when policies materially change
- ☐ New hires are trained before they touch PHI, not weeks later
- ☐ A written sanctions policy exists for privacy and security violations, and staff know it applies to everyone
- ☐ Staff have had specific phishing and email-handling guidance, not just generic awareness slides

4. Business Associate Agreements

Every outside vendor that creates, receives, maintains, or transmits PHI on your behalf generally needs a signed Business Associate Agreement (BAA) before they touch that data. The gap is almost never the billing company you remembered -- it is the email provider, the cloud backup, the IT contractor, or the shredding service you forgot counts.

- ☐ A current vendor list exists naming every party that touches PHI
- ☐ Signed BAAs are on file for billing/clearinghouse, IT/managed services, EHR/practice-management vendor, and cloud or backup providers
- ☐ Email, e-fax, texting, and any messaging tool carrying PHI is covered by a BAA
- ☐ Document storage, shredding, and offsite records vendors have BAAs
- ☐ No PHI is sent through a free consumer tool (personal Gmail, consumer texting, consumer file-sharing) that will not sign a BAA

If a vendor will not sign a BAA, that is your answer about whether PHI should flow through them.

5. Access Controls and Technical Safeguards

Technical safeguards are generally addressed under 45 CFR 164.312. The small-practice failure mode is shared logins and access that never gets removed -- the front desk all signs in as 'frontdesk,' and the assistant who left in March can still get into the EHR.

- ☐ Every user has a unique login -- no shared accounts for the EHR or workstations
- ☐ Access is removed the same day someone leaves or changes roles
- ☐ Access levels are reviewed at least annually so people only see what their job needs
- ☐ Automatic logoff is enabled on workstations and the EHR after a short idle period
- ☐ An audit log is turned on, and someone occasionally actually looks at it

6. Encryption

Encryption is an addressable safeguard, which means if you choose not to encrypt you have to document why and what you did instead -- and for most small practices there is no good reason not to. A lost laptop that is encrypted is generally a non-event; the same laptop unencrypted can be a reportable breach.

- ☐ Laptops and desktops that store or access PHI have full-disk encryption turned on
- ☐ Phones and tablets that access PHI or practice email are encrypted and passcode-locked
- ☐ Backups (onsite and cloud) are encrypted
- ☐ Any PHI sent by email outside the practice goes through secure or encrypted email, not plain email
- ☐ USB drives and other portable media carrying PHI are encrypted or not used at all

7. Physical Safeguards

Physical safeguards are easy to overlook because they are not on a screen. Walk your own office at eye level: what can a patient in the waiting room or a delivery person at the desk actually see and reach.

- ☐ Front-desk and clinical monitors are angled or shielded so patients cannot read them
- ☐ Server, network gear, and any paper charts are in a locked room or cabinet
- ☐ Visitor and after-hours access to areas with PHI is controlled (locks, keys, or codes that get changed when staff leave)
- ☐ Old computers, copiers, and hard drives are wiped or destroyed before disposal, with a record
- ☐ Paper PHI is shredded (or held for a BAA-covered shredding vendor), never put in regular trash or recycling

8. Breach Notification Readiness

The Breach Notification Rule sets the clock the moment something goes wrong, and a small practice that has to invent a process during an incident loses days it does not have. A one-page incident response plan that names who does what is worth more than a thick binder no one has read.

- ☐ A written incident response plan exists and names who leads, who investigates, and who notifies
- ☐ Staff know exactly who to tell, the same day, if a device is lost or PHI may have been exposed
- ☐ You have a documented way to assess whether an event is a reportable breach
- ☐ Required notification timelines and recipients (affected individuals, HHS, and in larger events the media) are written down before you need them
- ☐ Lost-device, ransomware, and misdirected-PHI scenarios have at least a basic playbook

Do not promise notification timelines from memory in this worksheet -- confirm current requirements when you build the plan.

9. Patient Rights

The Privacy Rule gives patients enforceable rights, and access complaints are a common driver of HHS enforcement against small practices. The fixable gap is usually a vague or slow records-request process and a stale privacy notice.

- ☐ A current Notice of Privacy Practices is given to patients and posted where they can see it
- ☐ You have a written, timely process for patients to request and receive copies of their records
- ☐ Records-request fees, if any, are limited to what is generally allowed and are not used to discourage access
- ☐ Patients have a clear way to request amendments and an accounting of certain disclosures
- ☐ Front-desk and clinical staff know the basic patient-rights process, not just the Privacy Officer

Count every box you left unchecked. Those are your remediation priorities, ranked roughly in the order of these domains -- and if your Security Risk Analysis box is unchecked, that is always gap number one. When you are ready to close them, use the GetPracticeHelp directory to find HIPAA risk-analysis, healthcare-IT, and compliance providers who work with independent practices.

This is general informational content to help you spot gaps, not legal or compliance advice, and it does not create any obligation or guarantee of compliance. HIPAA requirements depend on your specific practice and change over time. Have a qualified compliance professional or healthcare attorney review your policies, your Security Risk Analysis, and your overall program.