

HIPAA Gaps Found -- The Order to Close Them

A prioritized remediation plan for solo and small medical and dental practices, highest-risk and cheapest-to-fix first

You ran a quick-check and found gaps. The next question is sequence: what to fix this week, what to schedule, and what an investigator asks for first. Work the tiers below in order. The single most common gap costs hours of your time, not dollars.

How to use this list

These tiers are ordered by risk-per-dollar, not by how the rule is written. Tier 1 items are the things investigators request first and the cheapest to close. Tier 3 items matter, but they rarely sink a practice on their own.

Assign one owner and one due date to each checked item. An item with no name next to it does not get done.

Item counts here are typical for a 1-5 provider practice; your scope may differ.

Tier 1 -- Do first (cheap, high-risk, the things investigators ask for)

Start here even if Tier 2 feels more urgent. A Security Risk Analysis is generally required under 45 CFR 164.308, and its absence is almost always the #1 finding. It costs hours, not dollars -- you are documenting what you already know about where protected health information (PHI) lives and how it could be exposed.

- ☐ Complete or update a Security Risk Analysis covering every system that creates, receives, stores, or transmits PHI -- EHR, practice-management software, email, imaging, backups, and any laptop or phone. Date it and name who did it.
- ☐ List every vendor that touches PHI (EHR host, billing service, IT support, cloud storage, shredding, email provider) and confirm a signed Business Associate Agreement (BAA) is on file for each. No signed BAA means stop sending PHI until you have one.
- ☐ Confirm full-disk encryption is ON for every laptop, desktop, tablet, phone, and removable drive that can reach PHI. Encryption is an addressable specification under the technical safeguards at 45 CFR 164.312 -- if you do not encrypt, you must document why and what you do instead.
- ☐ Confirm email carrying PHI is encrypted or sent through a secure portal, not plain Gmail or Outlook to outside parties.
- ☐ Eliminate shared logins. Every person who touches the EHR gets a unique user ID so actions trace to an individual.

If you fix only one thing this month, fix the Risk Analysis -- it drives every other priority.

Tier 2 -- Foundational policies and training

Tier 1 closes the gaps that get cited. Tier 2 builds the paper trail that proves the gaps stay closed. These take days, not hours, and most can be done from templates you then adapt to how the practice actually runs.

- ☐ Put your HIPAA policies in writing -- Security, Privacy, and Breach Notification -- and store them where staff can find them. Generic templates are fine as a starting point; edit them to match your real workflows.
- ☐ Run workforce training at hire and at least annually, and collect a dated sign-off sheet from every person, including providers and the owner.
- ☐ Adopt a written sanction policy stating the consequences for violations, and apply it consistently.
- ☐ Review who has access to what at least annually. Cut access that no longer matches a person's job.
- ☐ Write a termination checklist that disables EHR, email, and building access the same day someone leaves, and run it every departure.

Tier 3 -- Operational hardening

These items reduce the odds of an incident and shorten your response when one happens. Schedule them over the quarter after Tier 1 and Tier 2 are in place.

- ☐ Write an incident-response and breach plan with concrete timelines, including who decides whether a breach is reportable and the notification deadlines you must meet.
- ☐ Fix physical safeguards: angle or privacy-screen monitors away from waiting areas, lock rooms holding records or servers, and limit facility keys and badges to current staff.
- ☐ Set a media-disposal rule: shred paper PHI and wipe or destroy drives, phones, and copiers before they leave the building.
- ☐ Document your patient-access procedure -- how someone requests their records, your turnaround, and what you may charge.
- ☐ Schedule the next re-assessment now so it does not slip.

Track it on one page

Tier	Focus	Typical effort	Owner
1	Risk Analysis, BAAs, encryption, unique logins	Hours to a few days	Owner / IT
2	Written policies, annual training, access and termination	Days	Owner / office manager
3	Incident plan, physical safeguards, disposal, access procedure	Days, spread over a quarter	Office manager

Keep this table with the date each item was completed -- a dated record is what you show when asked.

Set the cadence

HIPAA compliance is not a one-time project. Re-run the Security Risk Analysis after any major change -- a new EHR, a new location, a merger, a switch to telehealth -- and at least once a year regardless.

Put a recurring annual reminder on the calendar now, attached to a date you will not forget, such as license-renewal season. Re-confirm training sign-offs, access reviews, and your vendor BAA list on the same cycle.

Closing these gaps -- a current Risk Analysis, vendor BAAs, encryption, written policies -- often needs outside help. Find vetted HIPAA compliance and healthcare-IT providers in the GetPracticeHelp directory.

This is general informational content, not legal or compliance advice. HIPAA requirements depend on your practice's specifics, and rules change. Have a qualified compliance professional or healthcare attorney validate your program before relying on it.