MY DIGITAL LIFE · PORTLAND, OR

The Behavioral Health Practice HIPAA & IT Security Checklist

For solo and small-group practices in Oregon

The items a generalist IT provider will not check for you.

WHAT'S INSIDE

52
checklist items

10
focused sections

~30
minutes to run through

Including:

- The documentation HIPAA requires that most solo practices skip
- BAAs — the vendor list you probably have not audited
- Email, texting, and client communication gotchas
- Oregon-specific breach notification and records rules
- A 42 CFR Part 2 callout if your practice treats any SUD

Last updated April 2026 · my-digital-life.com

Before you start

This checklist is written for Oregon behavioral health practices with roughly one to ten clinicians — solo therapists, small group practices, and boutique psychiatric offices. It assumes your EHR is a modern SaaS platform (SimplePractice, TheraNest, Valant, or similar), that you run a small office or work from home, and that you do not have a full-time IT person on staff.

The goal is not to make you a HIPAA scholar. The goal is to surface the items a generalist "we handle small business IT" provider is statistically likely to miss, in a form you can run through once, then revisit quarterly.

A few items will not apply to every practice. Skip the ones that do not, check the ones that do, and circle the ones you are unsure about. The unsure ones are where the actual work is.

The ten sections:

SECTION 01

Required documentation you probably don’t have

HIPAA requires the paperwork even for a solo practice. The fact that no one checks does not mean it is not required.

- [ ] You have a written **HIPAA Security Risk Analysis** on file, completed in the last 12 months.
  Required under 45 CFR 164.308(a)(1). This is the single most-skipped requirement and the one OCR asks about first.
- [ ] You have a designated **Security Officer** and **Privacy Officer** in writing (even if it is just you).
  Both roles are required. They can be the same person. Put it in your policy document.
- [ ] You have written **HIPAA policies and procedures** that actually describe what your practice does.
  Not a downloaded template with "[Your Practice Name]" placeholders still in it.
- [ ] Every clinician and staff member has completed **HIPAA training** and you have a signed record of it.
  Annual refresh. Applies to you as the owner too.
- [ ] You provide every new client a **Notice of Privacy Practices** and have their signed acknowledgement on file.
- [ ] You have a written **Incident Response Plan** you could actually follow at 9pm on a Saturday.
  Three sentences is fine. Who do I call, what do I do first, what do I stop doing.

SECTION 02

Devices — laptops, desktops, phones

Anything that has ever touched client data is in scope. Personal and work.

- [ ] **Full-disk encryption** is enabled on every device that touches PHI (FileVault on Mac, BitLocker on Windows).
  Not "the EHR is encrypted." The device itself. Verify it is actually on — check in Settings, do not assume.
- [ ] Every device **auto-locks** within 5 minutes of inactivity and requires a password or biometric to unlock.
- [ ] **Operating system updates** are set to install automatically, and you have actually restarted recently.
- [ ] Every device has **endpoint protection** (antivirus or EDR) installed and running — not just the default Windows Defender that was never configured.
- [ ] Personal devices used for any practice work have a **separate user account** from family members, or are not shared at all.
- [ ] Mobile phones have a **PIN or biometric lock**, **remote wipe** enabled (Find My iPhone / Find My Device), and do not store client data in the Photos or Files app.

- [ ] No PHI is stored in **personal** iCloud, Google Drive, Dropbox, or OneDrive accounts — only in accounts your practice controls and has BAAs for.
- [ ] You have a written **inventory** of every device that touches PHI, including make, serial number, and who uses it.
  A spreadsheet is fine. The point is you could answer "what was on the stolen laptop" in under five minutes.

SECTION 03

Accounts, passwords, access

The cheapest, highest-impact layer. Most breaches at small practices start here.

- [ ] **Multi-factor authentication (MFA)** is enabled on your EHR, email, cloud storage, telehealth platform, and any account that touches client data. No exceptions.
  SMS texts count as MFA in a pinch. An authenticator app or hardware key is better.
- [ ] You use a **password manager** (1Password, Bitwarden, Dashlane) and every clinical account has a unique, long password generated by it.
- [ ] Every staff member has their **own login** to every system. No shared accounts, no "we all use the front desk password."
- [ ] When a staff member or contractor leaves, you have a **written offboarding checklist** that removes their access from every system the same day.
- [ ] You know **who has admin access** to your EHR and email tenant, and the list is no longer than it needs to be.

SECTION 04

Email, texting, and client communication

This is where small practices lose PHI most often, and where clients complain first.

- [ ] Your email is on a **HIPAA-compliant platform with a signed BAA** (Google Workspace with BAA, Microsoft 365 with BAA, or a healthcare-specific provider). A free Gmail or Yahoo address is not compliant.
- [ ] You have a **written policy** for what staff will and will not put in an email — and you follow it.
- [ ] Clinicians do **not text clients** from personal cell phones about clinical matters. If you text clients at all, you use a BAA-covered secure messaging tool (Spruce, OhMD, your EHR's secure messaging, etc.).
- [ ] Clients sign a **written communication preferences form** that captures what channels they consent to and documents the risks of each.
- [ ] Appointment reminders through your EHR have been **configured to not include identifying clinical information** (no diagnosis, no "group therapy," no provider specialty in some cases).
- [ ] If you still use fax, it is a **HIPAA-compliant eFax service with a BAA**, not a physical fax machine in a shared hallway.

- [ ] Voicemail greetings on any number clients use do **not identify the practice as behavioral health** in a way clients did not consent to — and you have a process for confirming voicemail is an OK channel before leaving one.

SECTION 05

EHR, telehealth, and vendor BAAs

Every third party that touches, stores, or transmits PHI needs a signed Business Associate Agreement. Every one.

- [ ] You have a **signed, current BAA on file** with your EHR vendor.
- [ ] You have a signed BAA with your **email** provider (and you have confirmed the specific plan you are on supports a BAA — many free tiers do not).
- [ ] You have a signed BAA with your **telehealth** platform — and if you use plain Zoom, FaceTime, or Google Meet, you have either a BAA or a documented plan to switch.
  "Zoom" and "Zoom for Healthcare" are different products. Check which one you are actually paying for.
- [ ] You have a signed BAA with your **cloud storage** provider if you store any PHI there outside the EHR.
- [ ] You have a signed BAA with your **billing service, clearinghouse, or medical biller**.
- [ ] You have a signed BAA with your **answering service** or virtual receptionist, if you use one.
- [ ] You have **reviewed the audit log** in your EHR at least once in the last 90 days and would recognize unusual activity if you saw it.

SECTION 06

Backups and ransomware readiness

If the answer to “when was the last time you restored from backup” is “we’ve never had to,” you don’t actually know if your backups work.

- [ ] Your EHR vendor’s backup story is **in writing** — you know their RPO (how much data could be lost), RTO (how long recovery takes), and what you are responsible for vs. what they are.
- [ ] Any PHI stored outside the EHR is backed up **somewhere the ransomware can’t reach** — immutable cloud backup, offline copy, or equivalent.
- [ ] You have **actually performed a test restore** of something in the last 12 months and verified the restored data opens correctly.
- [ ] You have a **cyber insurance policy** you have read, and you know what it requires of you (MFA, EDR, training) for claims to be honored.
  Most 2024+ policies have prerequisites. If you do not meet them, a claim gets denied.

SECTION 07

Your office and home network

The router matters more than most people realize — especially for telehealth providers working from home.

- [ ] Your office (or home office) Wi-Fi uses **WPA2 or WPA3 encryption** and a password that is not “password123” or the name of your practice.
- [ ] You have a **separate guest Wi-Fi network** for clients, visitors, and personal household devices. Your work devices never connect to the guest network and vice versa.
- [ ] Your router’s **admin password** has been changed from the factory default, and the firmware has been updated in the last year.
- [ ] If you work from home, your **household smart devices** (Ring, Nest, smart TVs, kids’ gaming consoles) are on a separate network from your work devices.
- [ ] If you have an in-office server or NAS, it is **physically secured**, not sitting under a waiting-room chair.

SECTION 08

If a breach happens

You do not need a perfect plan. You need a plan that exists before you need it.

- [ ] You know the **60-day HHS breach notification rule** exists and you know where your written procedure lives for handling it.
- [ ] You have the phone number for a **healthcare attorney licensed in Oregon** saved somewhere you can find it at 9pm.
- [ ] You know who your **cyber insurance incident response hotline** is — many policies require you to call them *before* calling your own IT person.
- [ ] You have a **communication template** for notifying affected clients, drafted in advance, reviewed by an attorney.

If your practice treats any substance use disorder, keep reading.

42 CFR Part 2 is a separate federal rule that sits **on top of** HIPAA for records identifying a patient as having a substance use disorder. Its consent and disclosure rules are stricter than HIPAA's, and the penalties are distinct. A generalist IT provider who says "we do HIPAA" is not the same as a provider who understands Part 2 record segregation, re-disclosure prohibitions, and the specific audit trail requirements the rule implies for your EHR configuration. If any of your clinicians diagnose or treat SUD — even occasionally — this applies to you.

SECTION 09

Oregon-specific items

Federal rules are not the whole picture. Oregon adds its own.

- [ ] You know that the **Oregon Consumer Information Protection Act** (ORS 646A.600–.628) requires breach notification to affected Oregonians and, above certain thresholds, to the Oregon Attorney General.
- [ ] If you receive client records from any **Oregon state-licensed mental health program**, you understand ORS 179.505 applies and your retention and disclosure obligations may be stricter than HIPAA alone.
- [ ] You retain mental health records for at least the **Oregon-required minimum** (generally 7 years for adult records, longer for minor records — confirm specifics with your licensing board).

SECTION 10

Annual and quarterly maintenance

The checklist is only useful if it gets run more than once.

- [ ] You have a **recurring calendar reminder** to re-run this checklist quarterly.
- [ ] You review and update your **HIPAA Security Risk Analysis** at least annually, and any time you add a major new system or vendor.
- [ ] You review your **BAA list** annually and confirm each agreement is still current and covers the products you are actually using (vendors rename and rebundle their offerings frequently).

You finished the list. What now?

If you walked through every item and every box is checked: congratulations — you are in a smaller group than you think. Put the checklist on your calendar for a quarterly review and get back to your caseload.

If a few items gave you pause, that is normal and it is fixable. The most common gaps we see in Portland behavioral health practices are missing Business Associate Agreements with at least one vendor, no written HIPAA Security Risk Analysis on file, personal devices touching client data without encryption or MFA, and backups that have never actually been test-restored to confirm they work. None of these are catastrophes if you address them before something goes wrong.

If the list made you realize you do not have an IT provider who actually understands behavioral health — not just "HIPAA in general," but the specific workflows, EHR platforms, and regulatory layers that apply to mental health and SUD practices in Oregon — that is what My Digital Life does.

A no-cost conversation, not a sales pitch.

Bring your checklist. We will walk through whatever is unchecked, tell you which gaps are urgent and which can wait, and send you a written summary. If we are a fit to help, we will say so. If you just need a nudge in the right direction, you will get that too.

my-digital-life.com · Portland metro, onsite and remote