DermHIPAA

The security checklist

Practice: _____ Checked by: _____ Date: _____

Nine areas, one at a time. For each, where to check it, then a box for each check. Some of it belongs to your IT company or your web company: give them their section, then go through it together. Tick each box as you go, date it, and keep it with your HIPAA records.

1. Domain security

Your domain (yourpractice.com) is the address behind your email and your website. Whoever controls it controls both.

Where to check it

Sign in to your domain registrar, the company you pay for the domain each year. Not sure which company that is? Look your domain up at https://lookup.icann.org/en/lookup. It shows your registrar, whether the domain is locked, and when it expires. If your web company set up your domain, ask them to sign in with you.

What to check

- ☐ Ensure the practice owns the login to your registrar, under an email address someone reads, and not a former employee or contractor.
- ☐ Ensure the registrar login has 2-step verification turned on.
- ☐ Ensure your domain is locked against transfers. On the ICANN lookup, "clientTransferProhibited" under Domain Status means it's locked.
- ☐ Ensure your domain is set to renew automatically, on a card that won't expire first.
- ☐ Ensure the login to your DNS host has 2-step verification too, if your DNS is managed by a different company than your registrar.
- ☐ Remove old DNS records, since leftover records pointing at services you no longer use can be taken over by someone else. Say survey.yourpractice.com still points at a survey service you cancelled: someone could claim that name on the service and put a fake login page on your own web address.

DermHIPAA

2. Email security

Email that pretends to come from your practice can fool your patients, your staff and your bank. A few public records on your domain decide whether most mailbox providers let it through.

Where to check it

Run your domain through our free email check at https://check.dermhipaa.com. It reads your public email records and explains each one in plain words. You don't need to sign in or give us an email address.

What to check

- ☐ Ensure you have one SPF record, not two, since two break each other. It should list every service that sends email as you, and nothing you've stopped using, and end in ~all.
- ☐ Turn on DKIM for Google Workspace and for every other service that sends email as you. Each gives you a key to add to your DNS as a TXT record. In Google Workspace it's at Admin console → Apps → Google Workspace → Gmail → Authenticate email: generate the key, add it to your DNS, then click Start authentication.
- ☐ Ensure your DMARC record is at p=reject, or on its way there, so most mailbox providers turn away email forged with your address, or send it to spam.
- ☐ Ensure your DMARC record asks only for aggregate reports (rua), not forensic ones (ruf), which can carry message subjects that name a patient. You don't want your DMARC reports to cause a HIPAA breach.
- ☐ Ensure whoever pays your bills confirms any new or changed bank details by calling a number they already have, never one in the email. AI can now imitate a voice from a short recording, so a call that sounds like the owner isn't proof either.

DermHIPAA

3. Google Workspace security

Google Workspace holds your email, your files and your staff's accounts. Most of what keeps it safe comes down to settings someone has to turn on.

Where to check it

Sign in to the Google Admin console at https://admin.google.com, as a super administrator. If your IT company runs it, ask them to share their screen and go through this with you. Each step below says where to click.

On Microsoft 365 instead? The same checks apply, in different places: most are in the Microsoft 365 admin center (https://admin.microsoft.com), Microsoft Entra (https://entra.microsoft.com) and Microsoft Defender (https://security.microsoft.com). Ask your IT company to go through this section with you there. The steps below are Google's, because Google Workspace is what we work in.

What to check

- ☐ Ensure Google's business associate agreement (BAA) is accepted: Account → Account settings → Legal and compliance.
- ☐ Ensure 2-step verification is enforced for everyone, not just allowed, and that the exception group is empty: Security → Authentication → 2-Step Verification.
- ☐ Ensure your administrators sign in with a security key or an authenticator app, never a text message.
- ☐ Keep to two or three super administrators, each with a separate account used only for admin work: Account → Admin roles → Super Admin.
- ☐ Ensure everyone has their own account, with no shared logins such as frontdesk@ or billing@ (turn those into Google Groups instead): Directory → Users.
- ☐ Remove access the same day someone leaves: Directory → Users. See when it happened in Reporting → Audit and investigation → User log events.
- ☐ Ensure each person can reach only what their job needs, through organizational units and groups: Directory → Organizational units, and Directory → Groups.
- ☐ Give your IT company its own account with a limited role, such as Google's Help Desk Admin, instead of a shared password: Account → Admin roles.
- ☐ Review every outside app that can reach your accounts, and block the ones nobody approved: Security → Access and data control → API controls → Manage Third-Party App Access.
- ☐ Ensure Drive files can't be shared outside the practice without a warning (or at all, if you can): Apps → Google Workspace → Drive and Docs → Sharing settings.
- ☐ Set sessions to end after a set time, so a forgotten sign-in doesn't stay open: Security → Access and data control → Google session control. (This needs Google Workspace Business Plus or higher.)

- ☐ Ensure phones that get practice email have a screen lock, and that you can wipe the practice account from a lost one: Devices → Mobile & endpoints → Settings.
- ☐ Ensure alerts from Google's Alert Center go to someone who reads them every business day: Security → Alert center.
- ☐ Review the sign-in log every month and write down what you found: Reporting → Audit and investigation. Google keeps these logs for six months, so ensure someone saves them for longer. HIPAA requires you to keep the records of your security reviews for six years.

DermHIPAA

4. Website security

AI tools are now finding flaws in website software faster than ever. A site that isn't kept up to date is one of the easiest ways in.

Where to check it

Ask your web company, or sign in to your web host's dashboard. If your site runs on WordPress, sign in at yourpractice.com/wp-admin and open Plugins.

What to check

- ☐ Ensure your website is on a managed host, so professionals keep the server it runs on secure. When October's PHP flaws were announced, managed hosts such as Pressidium, which runs our own sites, patched every site they host right away. Your site itself and its plugins are still yours to keep secure (below).
- ☐ Ask your host which PHP version runs your site, and ensure it's patched for October's flaws (CVE-2026-109618 and CVE-2026-109619): version 8.2.35, 8.3.36, 8.4.27, 8.5.12 or later. Anything on 8.1 or older needs upgrading.
- ☐ Update your plugins and themes; delete the ones you don't use.
- ☐ Ensure nothing on your site came from a website offering paid plugins for free.
- ☐ Update the UpdraftPlus backup plugin, if your site uses it, and ask your web company to look for plugins and administrator accounts nobody added. The update doesn't remove anything attackers already installed.
- ☐ Ensure any form that collects health or patient information, such as an appointment request, uses a company that has signed a BAA with you. Otherwise, take the health questions off the form.
- ☐ Keep a copy of your site somewhere other than your host.

DermHIPAA

5. Password security

One reused password can open every account that shares it. And an AI assistant signed in to the wrong place can see more than you meant to show it.

Where to check it

Open your team's password manager. In 1Password, Watchtower shows passwords that are reused, weak or in a known breach. To check whether an email address has turned up in a data breach, look it up at https://haveibeenpwned.com. Your IT company sets these tools up.

What to check

- ☐ Ensure everyone at the practice uses a password manager, such as 1Password, which we use ourselves.
- ☐ Ensure no password is used twice, and none sit in a spreadsheet, a note or on a sticky note.
- ☐ Move passwords saved in personal browser profiles into the password manager. They leave when the person does, and password-stealing malware looks for them.
- ☐ Change any password that has turned up in a known breach.
- ☐ Turn on 2-step verification everywhere it's offered: email, the bank, payroll, the EHR and your domain registrar.
- ☐ Ensure no AI assistant has a login to anything holding patient information unless its maker has signed a BAA with you that covers the feature you're using. A tool (such as 1Password) that hides the password from the assistant doesn't hide the patient information it sees once it's signed in.

DermHIPAA

6. Computer security

Every computer at the front desk, in an exam room or at home is a way into your practice.

Where to check it

Ask your IT company, which usually sees all of this from one dashboard. To check a single computer yourself:

- On Windows: Settings → Privacy & security → Device encryption (or search for BitLocker), and Settings → Windows Update.
- On a Mac: System Settings → Privacy & Security → FileVault, and System Settings → General → Software Update.

What to check

- ☐ Ensure updates install automatically, and that someone confirms they did.
- ☐ Replace or upgrade any computer still on Windows 10, which stopped getting free security updates in October 2025, or enroll it in Microsoft's paid Extended Security Updates while you plan.
- ☐ Ensure every computer runs business antivirus that your IT company manages, such as Bitdefender, which we use ourselves.
- ☐ Ensure every laptop and desktop has full-disk encryption turned on. Under HHS's guidance, a lost computer encrypted to its standard generally isn't a breach you have to report.
- ☐ Ensure screens lock after a few minutes.
- ☐ Ensure nobody uses an administrator account for everyday work.
- ☐ Ask your IT company which remote-access tools are installed on your computers, and ensure each is up to date and protected by 2-step verification.

DermHIPAA

7. Network security

Your router is the front door to everything in the office.

Where to check it

Ask your IT company, or your internet provider if it supplied the router. The router's own admin page is usually printed on a sticker on the router.

What to check

- ☐ Change the router's admin password from the one it came with.
- ☐ Ensure the router still gets updates from its maker, and replace it if it doesn't.
- ☐ Ensure patients' guest Wi-Fi is separate from the staff network.
- ☐ Ensure no computer can be reached from the internet by remote desktop. Remote access should go through a VPN or a remote-access tool with 2-step verification.

8. Backups

A backup is what gets you running again after ransomware, a mistake or a failed drive, but only if it works.

Where to check it

Open your backup service's dashboard, or ask your IT company. Google Workspace needs a backup of its own: a service you subscribe to that signs a BAA with you, such as IDrive, or a Synology storage device (a NAS) that you own.

What to check

- ☐ Ensure Google Workspace is backed up, and so is anything still on an office computer.
- ☐ Ensure your backup service has signed a BAA with you, since it holds a copy of your patient information.
- ☐ Keep at least one copy where ransomware can't reach it: offline, or in a backup that can't be changed or deleted.
- ☐ Restore a file from the backup at least once a year, and write down that it worked.

DermHIPAA

9. Cyber insurance

When something goes wrong, your cyber insurance should pay for the recovery. But an insurer can refuse to pay, or even cancel the policy, if its security requirements weren't met or something you told it wasn't true.

Where to check it

Your policy and the application you signed, both from your insurance broker.

What to check

- ☐ Re-read your application, and ensure every "yes" on it is still true today. In a 2022 case, an insurer went to court to cancel a $1 million policy after a ransomware attack, saying the company had claimed multi-factor authentication it wasn't actually using. The policy was declared void.
- ☐ Ask your broker whether your limit would cover an investigation, telling your patients, and the revenue you'd lose while you recover.
- ☐ Ask whether the policy pays less, or nothing, if an attack used software that hadn't been updated.
- ☐ Ask whom you must call first if something happens, and whether the insurer requires its own response team.
- ☐ Keep a dated record of what's in place and when it was last checked. This checklist, ticked and dated, is a good start!

From the guide at https://dermhipaa.com/security-checklist/

Need help with your own security or compliance? Book 20 minutes with Sam Roberts at https://calendar.app.google/Uq34XYNjhSQPz27b8