

HIPAA Compliance Checklist for Clinics

Does HIPAA apply to your clinic?

Tick the boxes that are true for your clinic.

- ☐ We provide health care to patients.
 - ☐ We send health information electronically for insurance or payment, for example insurance claims. This still counts if a billing company sends them for us.
-

Both boxes ticked? HIPAA applies to your clinic. Use the checklist below.

Not sure? Use the free [HHS tool](https://hhs.gov/hipaa/for-professionals/covered-entities) to check (hhs.gov/hipaa/for-professionals/covered-entities). Please do not decide your clinic is exempt from this quick check alone.

Our HIPAA checklist for clinics

This checklist covers the main HIPAA rules for clinics: the Privacy Rule, the Security Rule and the Breach Notification Rule. Tick each box your clinic can honestly say yes to. Any box you cannot tick is a gap to fix.

Some HIPAA steps are called "addressable." This does not mean optional. You must do them, or write down why they do not fit your clinic and use another measure that protects patient data just as well. Items marked "good practice" are not written in the law, but are widely recommended.

1. Set up responsibility

- ☐ Name a Privacy Officer and a Security Officer. In a small clinic, one person can do both jobs.
 - ☐ Write down policies for privacy, security and breach response.
 - ☐ Make a map of where patient information is kept and where it travels (EHR, email, phone, fax, cloud tools, paper files, clinical photo app). This is good practice and makes your risk check easier.
 - ☐ Keep all HIPAA documents for at least 6 years.
-

2. Find and reduce risks

- ☐ Do a written risk analysis. This means listing where patient data could be lost, stolen or seen by the wrong person.
 - ☐ Make a plan to fix each risk, and note who will do it and by when.
 - ☐ Repeat the risk analysis regularly and after big changes, such as a new system or a new office. Once a year is a common choice.
-

3. Train your team

- ☐ Train every staff member when they join, and again when your policies change. Many clinics also repeat the training every year (good practice).
 - ☐ Keep a record of each training: who took it and when. Asking each person to sign is a simple way to do this.
 - ☐ Write a clear rule for what happens if staff break the policies, and apply it.
-

4. Follow the Privacy Rule

- ☐ Give every new patient your privacy notice (called the Notice of Privacy Practices) at their first visit. Ask them to sign that they got it, and post the notice in your clinic and on your website. Keep it up to date.
 - ☐ Use and share only the minimum patient information needed for each task. Sharing for treatment is the exception.
 - ☐ Get the patient's signed permission before you use their information for marketing (for example, a post with their name, photo or story) or for anything else HIPAA does not already allow.
 - ☐ Let patients see their records and get a copy. Reply within 30 days.
 - ☐ Let patients ask you to fix mistakes in their records. Reply within 60 days.
 - ☐ Let patients ask for a list of the times you shared their information outside care, billing and daily clinic work (last 6 years). Reply within 60 days.
 - ☐ Have a way for patients to make a privacy complaint, and keep a record of each one. Never punish a patient for complaining.
 - ☐ Check the identity of anyone asking for patient information, unless you already know them.
-

5. Protect electronic patient information (Security Rule)

ADMINISTRATIVE

- ☐ Give each staff member only the access their job needs.
- ☐ Remove a person's access as soon as they leave the clinic.
- ☐ Write a plan for emergencies: make regular backups, be able to restore lost data, and keep patient information safe while your systems are down.

PHYSICAL

- ☐ Lock server rooms, file rooms and cabinets.
- ☐ Place screens so patients cannot see them. Use automatic screen locks.
- ☐ Wipe or destroy old computers, phones and drives safely.

TECHNICAL

- ☐ Give each staff member their own login. Never share passwords.
- ☐ Check that the person logging in is who they say they are. This is a HIPAA requirement. A strong way to do it is two-factor authentication.
- ☐ Encrypt patient information stored on laptops, phones and backups, and when it is sent by email. Encryption scrambles the data so only people with the key can read it. A screen password is not encryption. HIPAA calls encryption "addressable": do it, or write down why another way protects the data just as well.
- ☐ Keep a record of who opens each patient file, and check it regularly.
- ☐ Install software updates and security fixes on time (good practice).

6. Sign agreements with vendors

- ☐ List every vendor that touches patient data (EHR, billing, cloud storage, IT support, texting or clinical photo app).
- ☐ Sign a Business Associate Agreement (BAA) with each one before they get any patient data.
- ☐ Review these agreements regularly (good practice).

7. Be ready for a breach

- ☐ Write a plan for what to do if patient data is lost or seen by the wrong person.
 - ☐ Tell staff how to report a problem right away.
 - ☐ For every incident, write down what data was involved, who saw or got it, whether it was really seen or taken, and how much you reduced the risk. Unless you can show a low chance that the data was compromised, treat it as a breach.
 - ☐ If it is a breach, tell the affected patients without unreasonable delay, and no later than 60 days after you find it. This applies to unsecured data (data that was not properly encrypted or destroyed).
 - ☐ Tell HHS (the US health department) too. If 500 or more people are affected, do it at the same time as you tell the patients, and no later than 60 days after you find the breach. If fewer than 500 are affected, keep a log. You can report these to HHS at any time, but no later than 60 days after the end of the year you found them (about March 1).
 - ☐ Tell prominent media outlets in your state (such as newspapers, TV or radio stations) if more than 500 residents of that state are affected. Do this within 60 days after you find the breach.
 - ☐ Keep records of every incident, even small ones that did not need a report.
-

8. Keep it going

- ☐ Review your policies, risks and vendor list regularly. Once a year is a common choice.
 - ☐ Check regularly that staff follow your policies and that the policies still meet HIPAA. Once a year is a common choice.
 - ☐ Update your documents whenever HIPAA rules or your systems change.
-

Important: This checklist is a practical review aid, not legal advice, a certification or a guarantee of HIPAA compliance. Requirements depend on your clinic's circumstances. Confirm applicable obligations using official HHS guidance and qualified legal advice when needed.

Source: CureCast

<https://dr.curecasthealth.com/blog/hipaa-compliance-checklist-for-clinics/>

You are free to share this checklist. If you post it online, please add a link back to the source above.