HIPAA-Compliance Checklist

Published November 16, 2023

Download for free today

Download now

TABLE OF CONTENTS

If you're a therapist or clinician, you're undoubtedly familiar with the Health Insurance Portability and Accountability Act (**HIPAA**).

HIPAA compliance requirements encompass the legally bound ethical practices healthcare workers must abide by. To make sure you're staying compliant, we've come up with a HIPAA compliance checklist.

"HIPAA provides the minimal standard for protecting and sharing protected health information (PHI)," says Courtney Hebdon, LCSW, Director of Clinical Quality and Client Safety at **Thriveworks**.

"It is the guidance that all healthcare providers in the U.S. must follow to protect PHI and attempts to strike a balance between the efficient sharing of clients' healthcare information and the requirement to maintain confidentiality and data security," explains Hebdon. "It also governs a client's access to their own medical record and ensures that clients are informed of how their most sensitive information will be used and shared."

Under HIPAA regulations, therapists and clinicians are considered "**covered entities**"—and, as such, are required to comply with all HIPAA requirements.

But staying on top of **HIPAA compliance requirements** is a big job—and if you don't have a clear idea of what you need to be doing to comply, it's easy for things to fall through the cracks.

That's where a HIPAA compliance checklist can come in handy.

Using a HIPAA compliance checklist can ensure that you're doing everything you need to do to comply with HIPAA regulations—and are protecting both your clients and yourself.

But why is HIPAA compliance so important? As a clinician, what steps do you need to take to comply with HIPAA requirements? And what, exactly, do you need to include on your HIPAA compliance checklist?

Let's take a look at everything you need to know to ensure you and your practice are HIPAA-compliant.

Why is HIPAA compliance so important?

Before we jump into what to include in your HIPAA compliance checklist, let's quickly touch on why HIPAA compliance is so important.

"HIPAA compliance is a legal requirement for healthcare providers," says Hebdon. "It really serves to codify the ethical obligation of confidentiality, required by all healthcare license types."

In addition to upholding ethical standards, HIPAA compliance is also extremely important for therapists and clinicians because non-compliance can have serious consequences.

"There are federal and state consequences for non-compliance with HIPAA, from fines to criminal proceedings, reputational damage, and operational disruption, depending upon severity," says Hebdon. "Most companies also have internal consequences for violations as well, as do the various regulatory and licensing Boards."

What are the HIPAA compliance requirements?

Now that you understand the importance of HIPAA compliance, let's go into the HIPAA compliance requirements.

"HIPAA is multi-faceted in its requirements, covering general confidentiality and need for client/patient permission to disclose information," says Hebdon. "HIPAA also covers IT security and requirements for health record documentation security."

From a practitioner perspective, HIPAA is broken down into three main rules:

Privacy rule

"The Privacy Rule explains when, where, and how PHI can be shared," says Hebdon.

According to **HIPAA**, the Privacy Rule:

- Sets limits and conditions on use and disclosure of PHI.
- Requires health seekers' explicit authorization on any disclosures or uses of their PHI, outside protected entities, like their treating provider, health insurance payers, and healthcare workers.
- Gives individuals rights to get a copy of or examine their health records and PHI.

Security rule

"The Security Rule provides requirements for protecting PHI, especially electronic PHI," says Hebdon.

According to **HIPAA**, the Security Rule:

- Provides limits and protections around the access and use of PHI by covered entities.

- Ensures that PHI use and disclosures are limited to an as needed basis for protected entities.
- Establishes administrative, physical, and technical safeguards to prevent any mishandling of PHI and thwart any unauthorized access or security breaches.

Breach notification rule

"The Breach Notification Rule [describes] what a breach is, when and how any possible breach or violation of the Privacy Rule needs to be reported to the **Office of Civil Rights** (OCR), the enforcement authority for [the **U.S. Department of Health and Human Services**]," says Hebdon.

Compliance with all of these rules is a must for anyone considered a "covered entity"—which includes therapists, psychologists, and other clinicians.

HIPAA compliance checklist

Because HIPAA compliance is so important, you want to make sure that your practice is following all relevant HIPAA guidelines and regulations. A helpful tool to do that is a HIPAA compliance checklist.

Use this HIPAA security checklist—with recommendations from Hebdon—as a jumping

off point to ensure compliance:

1. Appoint an individual or individuals within your practice to oversee HIPAA compliance efforts—generally known as a Privacy Officer or Security Officer. Depending on your business structure, you may take this responsibility yourself.
2. Create policies and procedures to ensure HIPAA compliance (for example, **email procedures**).
3. Conduct regular audits and risk assessments—at least annually—to identify gaps and correct any compliance issues.
4. Ensure that all platforms (including EHR, telehealth platforms, client communication systems, and any other platforms that might interact with PHI) are HIPAA-compliant.
5. Implement basic recommended security measures to protect data and access to platforms. This includes two-factor authentication, strong passwords, virus protection, data encryption, etc.
6. Train staff members on how to handle PHI and navigate all relevant platforms.
7. Create a "**Notice of Privacy Practices**" document that outlines clients' privacy rights and how your practice handles PHI—and distribute it to all clients.
8. Create a Release of Information form for clients to request access to their PHI—or request access for a third-party.
9. Create a comprehensive process for identifying and investigating potential HIPAA violations, including incident tracking, reporting, and client notification protocols—as well as disciplinary measures for employees and/or business associates responsible for breaches.
10. Develop protocols on how to handle security breaches.
11. Review all relevant compliance policies with employees.
12. If necessary, consult with a HIPAA compliance expert to review and improve policies and procedures.

You can also download the free HIPAA compliance PDF to use in your practice. To learn more about HIPAA compliance, read our article on **What It Means to Be HIPAA Compliant**.

HIPAA compliance best practices

In addition to the HIPAA compliance checklist, here are a few best practices to keep in mind for running a HIPAA-compliant practice:

Educate yourself on HIPAA regulations—and stay on top of HIPAA changes

It's important to educate yourself on HIPAA regulations. One way to do this, for example, is by pursuing a HIPAA compliance certification.

While learning the rules is important, it's also "important to keep on top of any updates and changes to the rules," says Hebdon.

HIPAA compliance regulations can—and do—change. For example, "there are **currently new rules** being promulgated that will change the record request time from 30 days to 15—although it has not gone final yet," says Hebdon. So, if you want to ensure your practice is compliant, it's important to stay on top of any relevant changes.

Make sure your workplace is secure

A major element of HIPAA compliance is protecting client privacy. And part of protecting client privacy is making sure that your workplace is private—especially if

your workplace is a home office.

“It’s critically important to ensure your workspace is confidential,” says Hebdon. “Especially when working from home, ensuring the privacy of your clients should be a top priority.”

Take steps to secure your workplace and protect clients during sessions. For example, if you work from home or speak with clients on video sessions, make sure you’re in a quiet space and soundproof your office.

Report any breaches

No one wants to admit to making a compliance mistake. But if you (or someone in your practice) violates HIPAA regulations, it’s important that you **report the breach** immediately, or you could find yourself facing serious consequences.

“When a HIPAA breach occurs, it must be reported to the OCR,” says Hebdon. “Consequences include fines, and possible jail time depending on the situation. The fines can be quite hefty. States have comparable rules for which there may be consequences as well, including state licensure boards when it comes to breaching a client’s confidentiality.”

SimplePractice is **HITRUST certified**, which is the gold standard of security certifications in the healthcare industry. Learn more about all the ways we keep customer and client data safe on our **security page**.

Disclaimer: This article is for informational purposes only, and should not be considered legal or ethical advice. For specific guidance, consult with an attorney or your professional liability insurer.

How SimplePractice streamlines running your practice

SimplePractice is HIPAA-compliant practice management software with everything you need to run your practice built into the platform—from booking and scheduling to insurance and client billing.

If you've been considering switching to an EHR system, SimplePractice empowers you to streamline appointment bookings, reminders, and rescheduling and simplify the billing and coding process—so you get more time for the things that matter most to you.

Try SimplePractice free for 30 days. No credit card required.

SHARE

TAGS

EHR SOFTWARE SECURITY & HIPAA

You may also like

How to Record a HIPAA-Compliant Group Clinic Voicemail Script

GUIDE

SimplePractice Guide to North Carolina HIE 2023 Mandate

GUIDE

HIPAA Breach Notification Letter Template

TEMPLATE

View all

SimplePractice

practice insights

Get the latest tips and resources, delivered straight to your inbox.

Email address →

By entering your email address, you are opting-in to receive emails from SimplePractice on its various products, solutions, and/or offerings. Unsubscribe anytime.

About our product +

For practitioners +

For clients +

Company +

Help & support +

Download on the App Store

GET IT ON Google Play

HIPAA Compliant

HITRUST CSF Certified

PCI Compliant