hireteem.com

How to Meet HIPAA's **Access Security Requirements**

A step-by-step action guide, **no compliance background needed**

HIPAA has required unique logins for every system that touches patient information since 2003. What has changed is enforcement, vendors like EyeMed are now actively requiring it. This workbook helps you audit what you have today, fix what needs fixing, and put a plan in place so you stay compliant going forward.

Phase 1 **Map Your Systems** 30–45 min

01 - List Every System That Accesses Patient Information

Open a blank document or grab a piece of paper. Write down every platform your practice logs into that shows, stores, or sends patient information. If you are unsure whether a system counts, include it, you can remove it later.

Common systems to include:

EHR / Practice Management	Epic, Cerner, Athenahealth, DrChrono, Kareo/Tebra, RevolutionEHR, Eyefinity, Compulink, Jane App
Insurance & Benefits Portals	Insurance & Benefits Portals EyeMed Provider Portal, VSP Vision, Availity, UnitedHealthcare, Cigna, Medicare/Medicaid portals
Billing & Clearinghouses	Change Healthcare, Availity, TriZetto/Cognizant, Office Ally, Waystar, Tebra
Scheduling & Patient Engagement	Zocdoc, Phreesia, Klara, Luma Health, Nexhealth, Solutionreach, OfficeMate
Communication Tools	Weave, Mango Voice, RingCentral, TigerConnect, Updox
Other	Any platform your team logs into that displays or processes a patient's name, date of birth, insurance ID, or clinical notes

Phase 1 **Map Your Systems** 30–45 min

02 - Determine Who Needs Access to Each System

For each system on your list, think carefully about which roles truly require access to do their job, **not simply who has been using it.**

HIPAA's principle of minimum necessary access means a person should only have access to the systems, and the information within them, that they genuinely need to perform their specific duties. Giving access by default or out of convenience is not compliant.

Write down only the names or roles that have a genuine need for each system. This list becomes the basis for your audit in Phase 2.

Tip: *Include on-site staff and remote workers, anyone who logs in counts, regardless of where they work.*

Phase 2 **Audit Your Current Logins** 30–60 min

3 - Audit the Current State of Each System

Now go into each system's admin or user management settings and compare what exists today against the list of who *needs* access that you built in Step 2.

Document what you find. You are looking for three categories: **logins to keep** (individual logins that are already correct), **logins to create** (needed people with no individual login), and **logins to remove** (shared logins, or logins for people who no longer need access).

Tip: *Don't delete a shared login until you've confirmed everyone who needs access has their own working login. Sequence matters.*

4 - Brief Your Team

Before making any changes to your systems, let your team know what is happening and why. Keep it simple: shared logins are no longer permitted under HIPAA, and each person will soon have their own individual credentials.

Explaining the reason in advance, it is a federal requirement that protects your patients and your practice, avoids confusion when people receive new login invitations or find that shared credentials have been removed.

Share this workbook with anyone who has questions.

Phase 2 **Audit Your Current Logins** 30–60 min

5 - Create Individual Logins for Anyone Who Is Missing One

For every person on your needs list who does not yet have an individual login, go into the system's admin settings and create one.

- Use their name or work email as the username.
- Send each person their credentials directly, not through a group chat.
- Confirm they can log in successfully before moving to Step 6.

Tip: *Most platforms have an 'Add User' or 'Invite User' option under Settings or Admin.*

6 - Remove Shared Logins and Unnecessary Access

Once all individual logins are active and confirmed working, go back and disable or delete every shared login you identified in Step 3.

Do not leave shared logins active 'just in case.' An active shared login is a compliance gap, even if nobody is using it regularly.

Also remove access for anyone who was in the system but is not on your current needs list.

Phase 3 **Document and Stay Compliant** 15–20 min

7 - Create an Access Log

Create a simple spreadsheet: one row per person, one column per system. Mark which systems each person is authorized to access. This document serves as your audit trail. Keep it somewhere your office manager can access and update it whenever your team or systems change.

Tip: *Date-stamp it. If you are ever audited, showing a current, maintained access log demonstrates active compliance management.*

A note on what comes next

Completing this workbook puts your practice in compliance today. Staying compliant over time depends on onboarding and offboarding processes that treat system access as a built-in step, not something someone remembers on the way out the door.

That means defining who is responsible for provisioning and revoking access, and building that ownership formally into your processes. Having clear accountability for each system and each account is just as important as the work you did here.

Quick Reference **Checklist**

Print this page. Check each item off as you complete it.
When every box is checked, your practice is compliant.



Phase 1 Map Your Systems

- ☐ **Listed every system that accesses patient information**
  EHR, billing, insurance portals, scheduling, communication tools, clearinghouses
- ☐ **Determined who needs access to each system**
  Based on role and job function, not habit or convenience

Phase 2 Audit Your Current Logins

- ☐ **Audited the current login state of each system**
  Identified: logins to keep, logins to create, and logins to remove
- ☐ **Briefed the team on the change and the reason**
  Federal requirement, protects patients and the practice
- ☐ **Created individual logins for everyone on the needs list who was missing one**
  One account per person, name or work email as username
- ☐ **Confirmed each person can log in with their own credentials**
  Before removing any shared login
- ☐ **Removed all shared logins and unnecessary access**
  No active shared logins remaining

Phase 3 Document and Stay Compliant

- ☐ **Created an access log: who is authorized for which systems**
  Dated, accessible to your office manager, ready to update

Quick Answers to **Common Questions**

Who does this apply to?

Anyone who logs into a system that touches patient information, on-site staff, remote workers, and anyone else on your team, regardless of where they work.

Is this a new law?

No. The requirement has existed since 2003 under 45 CFR 164.312(a)(2)(i). What is new is that vendors like EyeMed are now actively enforcing it.

What happens if we wait?

Your team may find themselves locked out of portals on the day enforcement kicks in, unable to verify benefits, submit claims, or access records.

How long does this take?

Most practices can complete all three phases in one focused afternoon.

Do I need to redo this every year?

You do not need to redo the full audit annually, but your access log should be updated whenever someone joins, leaves, or changes roles.



Need support getting **your team compliant?**

Teem remote workers receive HIPAA compliance training through Teem University and arrive with structured onboarding built in. Schedule a free demo at **hireteem.com**

This workbook is for informational purposes only and does not constitute legal advice. Consult a qualified healthcare compliance attorney for guidance specific to your practice.

Created by Teem · May 2026