HIPAA COMPLIANCE CHECK · OCTOBER 2026

Is your business ready for HIPAA? 16 questions for business associates.

Answer each question about the HIPAA Security Rule safeguards that apply to companies handling patient data for healthcare clients. High-priority safeguards count for more. Total your score on the last page, then start with the high-priority gaps.

01
Answer
Questions drawn from the HIPAA Security Rule safeguards that apply to business associates — the companies that handle patient data for healthcare clients.

02
Score
The safeguards that come up most in investigations and client security reviews count most. Your grade updates as you go.

03
Fix
Get the gaps to close, most important first — and print or save them for your compliance file.

COMPANY _____ DATE _____

COMPLETED BY _____ REVIEWED WITH _____

866.24.CALIT info@calitgroup.com calitgroup.com/hipaa-compliance-check

01 Agreements & ownership

Who is responsible, which contracts cover PHI, and where that data actually lives.

1 Do you have a signed business associate agreement (BAA) with every healthcare client whose patient data you handle?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
A current BAA for each covered entity, filed where you can find it — plus BAAs with your own subcontractors that touch the data.

IF NOT, FIX IT
Get a signed BAA in place with every healthcare client and every subcontractor that creates, receives, stores or sends their PHI.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

2 Is one named person responsible for HIPAA security at your company?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
A designated security official who owns the program, keeps the documentation and answers client questionnaires.

IF NOT, FIX IT
Name a security official — a vCISO can fill this role if no one in-house has the time.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

3 Do you know everywhere PHI lives — systems, cloud apps, email, file shares and laptops?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
A written list of every place patient data is stored, processed or sent, kept up to date.

IF NOT, FIX IT
Map where PHI lives and flows, so every location is covered by your safeguards and your risk analysis.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

02 Risk analysis & policies

A documented risk analysis is the foundation of the Security Rule — and one of the most common gaps found in federal investigations.

4 Have you completed a documented HIPAA security risk analysis in the last 12 months?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
A written assessment of the threats to PHI in your environment, the likelihood and impact of each, and the plan to address them.

IF NOT, FIX IT
Complete a documented security risk analysis now, update it at least yearly and after major changes, and track the fixes it finds.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

5 Do you have written security policies and procedures, reviewed every year and kept for six years?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Policies for access, devices, incidents and contingency planning that match how you actually work — with older versions kept on file.

IF NOT, FIX IT
Write (or update) security policies that match your real practices, review them yearly and keep each version for six years.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

6 Are the cloud services that store PHI — email, file sharing, backup — covered by a BAA and set up for it?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
For example, Microsoft 365 under Microsoft's BAA with the right security settings turned on, and no PHI in personal or free accounts.

IF NOT, FIX IT
Move PHI into services that sign a BAA, configure them securely and keep it out of personal and free accounts.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

03 Access controls

Making sure only the right people can reach PHI, and that you can show who did.

7 Is multifactor authentication required for email, remote access and every system that holds PHI?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
A stolen password alone can't open a mailbox, the VPN or an app with patient data.

IF NOT, FIX IT
Require MFA on email, remote access and every application that stores PHI.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

8 Does everyone have their own login, with access removed the day someone leaves?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
No shared accounts, and a checklist that closes every account when an employee or contractor departs.

IF NOT, FIX IT
Give every person a unique login and make account removal part of your offboarding checklist.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

9 Is access to PHI limited to the people who need it for their job?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Role-based permissions on folders, apps and mailboxes, reviewed at least once a year.

IF NOT, FIX IT
Set role-based access to PHI and review who has it at least yearly.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

10 Are access logs for systems with PHI kept and reviewed?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
Sign-ins and access to patient data are logged, retained and checked for anything unusual.

IF NOT, FIX IT
Turn on audit logging for systems with PHI and have someone review the logs on a schedule.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

04 Devices & data

Protecting PHI on laptops, in email and in backups.

11 Are laptops, phones and portable drives that may hold PHI encrypted?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE
BitLocker or FileVault on every laptop and encryption on mobile devices — so a lost device is far less likely to become a reportable breach.

IF NOT, FIX IT
Encrypt every laptop and mobile device that may hold PHI and manage them centrally so a lost one can be wiped.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

12 Is PHI sent by email encrypted?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
A simple way for staff to send encrypted email, and a rule about when they must use it.

IF NOT, FIX IT
Set up email encryption and a clear rule for when PHI must be sent encrypted.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

13 Is every device protected by endpoint detection and response and kept patched?

Important · worth 4 points

WHAT GOOD LOOKS LIKE
EDR on every computer and server, watched around the clock, with security updates installed on a schedule.

IF NOT, FIX IT
Deploy managed EDR on every device and automate patching for operating systems and apps.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

14 Is PHI backed up, with a tested plan to restore it after an outage or ransomware?

Important · worth 4 points

WHAT GOOD LOOKS LIKE

Backups kept out of ransomware's reach, restores tested, and a written contingency plan for keeping the work going.

IF NOT, FIX IT

Back up PHI to a copy ransomware can't reach, test restores and write down your contingency plan.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

05 People & incidents

Training your workforce, and knowing exactly what to do — and who to tell — when something goes wrong.

15 Does everyone who handles PHI get security training when they start and every year after?

Important · worth 4 points

WHAT GOOD LOOKS LIKE

Training records you can show a client or investigator, plus phishing tests to back it up.

IF NOT, FIX IT

Train your workforce on HIPAA security at hire and yearly, and keep the completion records.

Our answer: ☐ Yes (4) ☐ Partly / not sure (2) ☐ No (0)

16 Do you have a written incident response plan that covers notifying your healthcare clients of a breach?

High priority · worth 6 points

WHAT GOOD LOOKS LIKE

Who investigates, who decides, and how you notify each client in the time your BAA requires — and never later than HIPAA's 60 days.

IF NOT, FIX IT

Write an incident response plan that includes your BAA notification deadlines, and walk through it with leadership once a year.

Our answer: ☐ Yes (6) ☐ Partly / not sure (3) ☐ No (0)

SCORECARD

Total your score.

Add the points for each area, out of 76. Any “No” on a high priority item is worth fixing first, whatever the total.

AREA	QUESTIONS	SCORE
01 · Agreements & ownership	3	/ 14
02 · Risk analysis & policies	3	/ 16
03 · Access controls	4	/ 18
04 · Devices & data	4	/ 18
05 · People & incidents	2	/ 10
Total	**16**	**/ 76**

A · 69+
Strong — keep the documentation current

B–C · 50+
Solid start, with gaps to close

D · 38+
Gaps a client review or investigation would find

F · under 38
Significant exposure — start with the fixes

WANT AN ENGINEER TO CHECK IT FOR REAL?

Want help closing the gaps?

Configured, not just installed
A self-check shows what’s in place. We check whether it’s set up well and actually monitored.

Plain-language report
We check each safeguard for real, complete your security risk analysis, put the technical controls in place and keep the documentation ready.

Discreet
We can work around your current provider and sign an NDA.

No obligation
Use the results with us, your current provider or anyone else.

Book at calitgroup.com/contact

866.24.CALIT

A general guide based on the HIPAA Security Rule — not legal advice, and not a certification.