COMPLIANCE CHECKLIST

HIPAA compliance checklist

Health Insurance Portability and Accountability Act

Jurisdiction: US healthcare (covered entities and business associates)

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who HIPAA applies to

US healthcare covered entities (health plans, healthcare clearinghouses, most healthcare providers) and their business associates that handle protected health information (PHI).

HIPAA checklist

STEP 1

- [ ] Run an accurate and thorough HIPAA risk analysis (45 CFR 164.308(a)(1)(ii)(A)).

STEP 2

- [ ] Maintain a current Notice of Privacy Practices and patient access workflow.

STEP 3

- [ ] Implement administrative, physical, and technical safeguards per the Security Rule.

STEP 4

- [ ] Execute Business Associate Agreements with every vendor that handles PHI on the covered entity's behalf.

STEP 5

- [ ] Train the workforce on privacy and security policies - initial onboarding plus annual refreshers.

STEP 6

- [ ] Document access controls - joiner / mover / leaver against every system that holds ePHI.

STEP 7

- [ ] Operate the Breach Notification Rule process (4-factor risk assessment + 60-day clock).

STEP 8

- [ ] Maintain a sanctions policy and disciplinary record for HIPAA violations.

STEP 9

- [ ] Document the contingency plan: backups, disaster recovery, emergency mode.

STEP 10

- [ ] Annual review of the risk analysis output and re-attest where required.

FAQ

Who has to comply with HIPAA?

Covered entities (health plans, healthcare clearinghouses, and most healthcare providers that transmit electronic transactions) and business associates that create, receive, maintain, or transmit PHI on behalf of a covered entity.

Is a HIPAA compliance checklist enough?

A checklist is the right starting point, but HIPAA compliance is operational - it lives in the processes that produce evidence year after year. Most enforcement actions begin not because the checklist was incomplete but because the underlying processes drifted. The diagram on this page is the cadence the OCR expects to see operating.

How often do I need to run a HIPAA risk analysis?

HIPAA does not prescribe a fixed frequency, but the OCR has consistently emphasised that the risk analysis must be "accurate and thorough" and refreshed in response to material changes (new systems, new business associates, incidents). In practice, most programmes run it annually and update for triggering events.

What is the difference between this and the "seven HIPAA processes" page?

This page is the line-by-line checklist for an organisation-wide HIPAA programme. The /hipaa-compliance-processes page goes deeper into the seven specific operational processes (breach notification, incident response, access management, BA onboarding, risk analysis, workforce training, ePHI disposal), with the breach-notification process rendered as an editable BPMN map and the remaining six catalogued for follow-up.

Source: https://ba-copilot.com/compliance/hipaa-compliance-checklist. Tick each item as it is completed and add the named owner.