

Requirements for Group Health Plans Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.314(b)(1) — Requirements for Group Health Plans

Issued	9 August 2026
Prepared by	HIPAA Auditors — certified HIPAA lead auditors
Contact	info@hipaaauditors.com · +91-95851-60363
Address	100 Congress Ave, Suite 2000, Austin, TX 78701

How to use this document. This is a working template, not a finished compliance artefact. Replace every bracketed placeholder with your organisation's own detail, delete the guidance notes, and have the result reviewed and formally adopted by your Privacy or Security Officer before you rely on it.

Regulatory basis. References are to the HIPAA Administrative Simplification regulations at 45 CFR Parts 160, 162 and 164, and to NIST SP 800-66 Rev. 2, *Implementing the HIPAA Security Rule*.

The requirement

Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to 164.504(f)(1)(ii) or (iii), or as permitted under 164.508(a)(3)(i), a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI.

45 CFR 164.314(b)(1) · Organizational Requirements

Risk level	Difficulty	Typical cost	Timeframe
High	Moderate	Medium	2-4 months

Implementation steps

	Except where the only ePHI disclosed to a plan sponsor is disclosed under 164.504(f)(1)(ii) or (iii), or as authorised under 164.508, a group health plan must ensure its plan documents require the plan sponsor to reasonably and appropriately safeguard ePHI it creates, receives, maintains or transmits on the plan's behalf. The requirement sits at 164.314(b)(1), and the specifications at 164.314(b)(2)
	Plan documents must require the plan sponsor to:
	Implement administrative, physical and technical safeguards that reasonably and appropriately protect ePHI
	Ensure that adequate separation between the plan and the plan sponsor, required by 164.504(f)(2)(iii), is supported by reasonable and appropriate security measures
	Ensure that any agent to whom it provides ePHI agrees to implement reasonable and appropriate security measures
	Report to the group health plan any security incident of which it becomes aware
	Implementation approach:
	- Identify precisely which ePHI flows to the plan sponsor and under what authority; enrolment and disenrolment information and summary health information carry different treatment
	- Amend plan documents to carry each required provision. This is a plan document obligation, not a business associate agreement, and the two are frequently conflated
	- Make the firewall between plan administration and employment functions real: restrict access to named individuals performing plan administration, and enforce it technically
	- Name the individuals or classes permitted access in the plan documents, and keep that list current
	- Train those individuals on their distinct obligations and record it
	- Establish an incident reporting route from the sponsor back to the plan
	- Flow the requirements to any agent or third-party administrator handling plan ePHI

	- Retain plan documents and amendments for six years under 164.316(b)(2)
	The recurring failure here is practical rather than legal: HR staff hold both employment and plan administration roles, and the separation exists on paper while the same person sees both sets of data with the same account

Evidence to produce and retain

Tick only where the artefact exists and you can say where it lives.

	Plan documents containing each provision required by 164.314(b)(2) Location: _____ Owner: _____
	Plan document amendments and their adoption records Location: _____ Owner: _____
	Description of ePHI flows between the plan, the sponsor and any third-party administrator Location: _____ Owner: _____
	Named individuals or classes permitted access for plan administration, kept current Location: _____ Owner: _____
	Adequate separation procedures and the technical measures enforcing them Location: _____ Owner: _____
	Access control configuration evidence showing the separation is enforced in systems Location: _____ Owner: _____
	Training records for individuals with plan administration access Location: _____ Owner: _____
	Agent and third-party administrator agreements carrying the requirements downstream Location: _____ Owner: _____
	Incident reporting procedure from sponsor to plan, and records of reports made Location: _____ Owner: _____
	Retention evidence for plan documents under 164.316(b)(2) Location: _____ Owner: _____

How this gets tested

These are the procedures an auditor is likely to run. Self-test first.

	Review plan documents and confirm every provision required by 164.314(b)(2) is present Result: _____ Tested by / date: _____
	Map actual ePHI flows and compare against the documented description Result: _____ Tested by / date: _____

	reality Result: _____ Tested by / date: _____
	Test access list of individuals permitted plan administration, enforced, not merely stated Result: _____ Tested by / date: _____
	Sample individuals holding both HR and plan administration duties and examine how their access is segregated Result: _____ Tested by / date: _____
	Confirm training was delivered to those with plan administration access, with records Result: _____ Tested by / date: _____
	Review agent and third-party administrator agreements for flow-down of the requirements Result: _____ Tested by / date: _____
	Trace any incident reported by the sponsor through to the plan's response Result: _____ Tested by / date: _____
	Confirm summary health information and enrolment data are handled under the correct authority Result: _____ Tested by / date: _____
	Verify plan documents and amendments are retained for six years Result: _____ Tested by / date: _____

Common failures to check yourself against

- Plan documents never amended to include the required security provisions
- A business associate agreement used in place of the plan document amendment, which does not satisfy the requirement
- Separation stated in policy while the same HR staff access plan and employment data with one account
- No current list of individuals permitted access for plan administration
- Plan ePHI held in general HR systems accessible to the whole HR function
- Agents and third-party administrators given plan ePHI without the requirements flowing down
- No route for the sponsor to report security incidents to the plan
- Plan administration staff receiving only general HIPAA training
- Summary health information treated as unrestricted

Beyond the minimum

- Enforce separation with distinct system roles and separate accounts, not just written policy
- Keep the list of permitted individuals short, named and reviewed at least annually
- Segregate plan administration data into a system or partition that employment-function staff cannot reach
- Train plan administration staff separately, because their obligations differ from general HIPAA training
- Review plan documents whenever the administrator, carrier or plan design changes
- Log access to plan ePHI and review it, particularly where staff hold dual roles
- Confirm third-party administrators carry the requirements to their own subcontractors
- Document the authority for each data flow so the 164.504(f) exceptions are applied deliberately

HIPAA Auditors

Requirements for Group Health Plans Implementation Checklist
<https://hipaaauditors.com>

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.4.2

Sign-off

Completed by	Title	Date
Reviewed by	Title	Next review due

Want this verified independently? We test controls like this one on every HIPAA engagement. Request a scoped quote at <https://hipaaauditors.com/contact>