HIPAA AUDITORS

Business Associate Contracts or Other Arrangements Implementation Checklist

Implementation and evidence checklist for 45 CFR 164.314(a)(1) — Business Associate Contracts or Other Arrangements

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

A covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

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

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

Implementation steps

	A covered entity may permit a business associate to create, receive, maintain or transmit ePHI on its behalf only with satisfactory assurances, documented in a written contract, that the business associate will appropriately safeguard the information. The organisational requirement at 164.314(a)(1) sets what that contract must contain; 164.308(b)(1) requires the assurances themselves
	The agreement must require the business associate to:
	Comply with the Security Rule's administrative, physical and technical safeguards
	Ensure that any subcontractor creating, receiving, maintaining or transmitting ePHI on its behalf agrees to equivalent restrictions, through a downstream agreement
	Report security incidents, including breaches of unsecured PHI, to the covered entity
	Make its practices available to HHS for compliance review
	Return or destroy PHI at termination where feasible, and extend protections where it is not
	Operating the requirement in practice:
	- Identify business associates by function, not by label. A vendor with incidental, unavoidable access — a cloud host, a managed service provider, an offshore transcription service — is a business associate. Conduit exceptions are narrow and often misapplied
	- Maintain a register with counterparty, service, ePHI involved, agreement dates, expiry and renewal owner
	- Execute the agreement before any ePHI moves, not after go-live
	- Set breach reporting timelines in the contract rather than relying on the regulatory default, which can consume most of your own 60-day window
	- Assess the risk each business associate presents proportionate to the data they hold; a signature is assurance, not verification
	- Track subcontractors where they materially hold your data
	- Review agreements on renewal, on material service change, and when regulation changes

- [ ] **- Ensure termination triggers return or destruction, and obtain confirmation**
- [ ] **Business associates are directly liable for Security Rule compliance and have been the subject of OCR enforcement in their own right**

Evidence to produce and retain

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

- [ ] **Business associate management policy and procedure**
  Location: _____ Owner: _____
- [ ] **Register of all business associates, with service, ePHI involved and access route**
  Location: _____ Owner: _____
- [ ] **Executed business associate agreements, with effective and expiry dates**
  Location: _____ Owner: _____
- [ ] **Evidence that the agreement predates any ePHI disclosure**
  Location: _____ Owner: _____
- [ ] **Subcontractor arrangements where a business associate uses downstream providers**
  Location: _____ Owner: _____
- [ ] **Risk assessment or due diligence records per business associate, proportionate to risk**
  Location: _____ Owner: _____
- [ ] **Breach and incident notification terms, including agreed timelines**
  Location: _____ Owner: _____
- [ ] **Renewal tracking and review records**
  Location: _____ Owner: _____
- [ ] **Termination records showing return or destruction of PHI, with confirmation received**
  Location: _____ Owner: _____
- [ ] **Records of incidents reported by business associates and the response taken**
  Location: _____ Owner: _____

How this gets tested

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

- [ ] **Reconcile the business associate register against accounts payable and the vendor list to find unregistered relationships**
  Result: _____ Tested by / date: _____
- [ ] **Confirm a signed agreement exists for every counterparty with access to ePHI**
  Result: _____ Tested by / date: _____
- [ ]

	Result: _____ Tested by / date: _____
	Review the agreement text for each data processor, including PHI disclosure flow-down and incident reporting Result: _____ Tested by / date: _____
	Sample cloud and IT vendors specifically, since these are most often misclassified as outside scope Result: _____ Tested by / date: _____
	Confirm breach notification timelines are contractually specified rather than left to default Result: _____ Tested by / date: _____
	Review due diligence evidence and test whether it is proportionate to the data held Result: _____ Tested by / date: _____
	Confirm expiring agreements are tracked and renewed before lapse Result: _____ Tested by / date: _____
	Sample terminated relationships and confirm PHI return or destruction was obtained in writing Result: _____ Tested by / date: _____
	Trace a business-associate-reported incident through to your own documented response Result: _____ Tested by / date: _____

Common failures to check yourself against

- No agreement in place with a vendor that clearly handles ePHI
- Agreement signed after the service went live and data had already moved
- Cloud and IT providers wrongly excluded on a mistaken reading of the conduit exception
- Agreements missing required terms, particularly subcontractor flow-down and incident reporting
- Breach notification left at the regulatory default, leaving no time for the covered entity to act
- No register, so nobody knows how many business associates exist
- Agreements lapsed and never renewed, with the relationship continuing regardless
- Due diligence limited to collecting a signature, with no assessment of actual safeguards
- No evidence of PHI return or destruction after termination
- Subcontractor chains entirely untracked

Beyond the minimum

- Keep a single register of business associates with named owners and automated expiry alerts
- Classify by function and data access rather than by vendor category or self-description
- Require breach notification well inside the regulatory default, so your own 60-day clock is protected
- Scale due diligence to risk: request SOC 2 Type 2 or HITRUST evidence from vendors holding large volumes of ePHI
- Make agreement execution a gate in procurement, before any data moves
- Reassess vendors periodically rather than only at onboarding
- Record subcontractor chains where your data materially sits downstream
- Build termination obligations into the contract and hold the confirmation of destruction
- Treat cloud infrastructure providers as business associates where they maintain ePHI, even encrypted

NIST mapping: NIST SP 800-66 Rev. 2: Section 3.4.1

Sign-off

Completed by	Title	Date
Reviewed by	**Title**	**Next review due**