PRACTICAL COMPLIANCE RESOURCE

Quick Guide: Creating and Reviewing a HIPAA BAA

A fillable checklist for evaluating Business Associate Agreements before PHI is shared.

Organization / Vendor:	Reviewer:
Review date:	Agreement status:

How to use this guide. Complete each section before onboarding or renewing a vendor that may create, receive, maintain, or transmit protected health information (PHI). Unchecked items should be resolved or documented before approval.

Reference: HHS Sample Business Associate Agreement Provisions

1. Confirm That a BAA Is Required

- ☐ The outside party will handle PHI on behalf of a covered entity or business associate.
- ☐ The vendor's actual access - not merely its job title - has been reviewed.
- ☐ All systems, services, integrations, and subcontractors that may handle PHI have been identified.
- ☐ The reason for requiring or not requiring a BAA has been documented.
- ☐ The BAA will be signed before PHI is shared.

2. Map the Service and PHI

- ☐ The services the vendor will provide are documented.
- ☐ The types and formats of PHI involved are identified.
- ☐ The locations where PHI will be stored and processed are known.
- ☐ The people and roles that can access the information are identified.
- ☐ The retention period is defined.
- ☐ Subcontractors and cloud providers that may handle PHI are identified.
- ☐ Any de-identification, aggregation, analytics, or reuse of data is expressly addressed.
- ☐ The process for returning or destroying PHI when the service ends is defined.

3. Verify the Required BAA Provisions

- ☐ Permitted and required uses and disclosures of PHI are clearly defined.
- ☐ Other uses and disclosures are prohibited unless required by law.
- ☐ Appropriate privacy and security safeguards are required.
- ☐ Applicable HIPAA Security Rule obligations are included.
- ☐ Improper uses, disclosures, security incidents, and breaches must be reported.
- ☐ Individual access, amendment, and accounting-of-disclosures obligations are supported.
- ☐ The business associate must comply when performing a Privacy Rule obligation for the covered entity.
- ☐ HHS access to relevant practices, records, and documentation is preserved.
- ☐ Applicable restrictions and safeguards flow down to subcontractors.
- ☐ PHI must be returned or destroyed at termination when feasible.

- ☐ Protections continue when return or destruction is infeasible.
- ☐ The covered entity may terminate the agreement for a material violation.

4. Review the Operational Terms

- ☐ Incident-reporting deadlines are specific and workable.
- ☐ The deadline gives the covered entity sufficient time to investigate and respond.
- ☐ The vendor may provide preliminary notice followed by additional details as they become available.
- ☐ Responsibilities for breach assessment and notification are assigned.
- ☐ Investigation, mitigation, and notification costs are addressed.
- ☐ Encryption, authentication, access controls, logging, backups, and recovery expectations are appropriate.
- ☐ Audit, assessment, and security-documentation rights are defined.
- ☐ Cybersecurity insurance, indemnification, and liability provisions have been reviewed.
- ☐ Data-return format and deletion-verification procedures are specified.
- ☐ The agreement identifies which document controls if terms conflict.

5. Evaluate Subcontractors

- ☐ The vendor has identified relevant subcontractors and subprocessors.
- ☐ Downstream parties must accept equivalent PHI restrictions and safeguards.
- ☐ The vendor remains accountable for subcontractor performance.
- ☐ Subprocessor changes require appropriate notice.
- ☐ The vendor can obtain information needed to investigate a downstream incident.
- ☐ Subcontractor data is covered by return and destruction requirements.

6. Check for Common Red Flags

- ☐ No clause gives the vendor overly broad rights to use data for general business purposes.
- ☐ Advertising, product development, analytics, or AI training is not permitted without clear authorization.
- ☐ The agreement includes specific obligations beyond a general promise to comply with HIPAA.
- ☐ The regulatory 60-day maximum is not being treated as the only incident-reporting standard without review.
- ☐ Subcontractors, backups, archives, exports, and test systems are not omitted.
- ☐ The vendor cannot retain PHI indefinitely without an authorized purpose.
- ☐ Data return or deletion is not merely optional.
- ☐ The BAA does not conflict with the service agreement, privacy policy, or security addendum.
- ☐ The agreement permits termination when continued PHI access would create unacceptable risk.
- ☐ Neither party is accepting responsibilities it cannot operationally perform.

7. Complete the Pre-Signature Review

- ☐ Privacy and compliance stakeholders have reviewed the agreement.
- ☐ Information security has evaluated the vendor and proposed safeguards.
- ☐ Operational owners have confirmed that the agreement matches the service.
- ☐ Qualified legal counsel has reviewed significant legal and financial provisions.

- ☐ Required vendor-risk assessments are complete.
- ☐ The correct legal entities are named.
- ☐ The BAA and underlying service agreement are ready to take effect together.
- ☐ Authorized representatives have signed the final agreement.

8. Manage the BAA After Signature

- ☐ The executed BAA is stored in a central agreement inventory.
- ☐ The agreement owner, effective date, and related service contract are recorded.
- ☐ Incidents, vendor changes, and new subprocessors are monitored.
- ☐ Access is reviewed periodically and removed when no longer needed.
- ☐ The BAA is reassessed when services, systems, data uses, or regulations change.
- ☐ The agreement is reviewed during contract renewals.
- ☐ PHI return or destruction is documented when the relationship ends.
- ☐ The agreement and supporting records are retained according to applicable requirements.

Final Approval Test

Before approval, every reviewer should be able to answer these four questions clearly:

- ☐ Exactly what PHI will the business associate handle?
- ☐ Exactly what may the business associate do with it?
- ☐ Exactly what happens if the information is exposed or misused?
- ☐ Exactly what happens to the information when the relationship ends?

> **Decision rule:** If any answer is unclear, the agreement is not ready to sign.

Reviewer Notes

Final disposition: ☐ Approve ☐ Revise ☐ Reject

Educational use only. This checklist is not a contract template or legal advice. Have qualified legal, privacy, and security professionals review each BAA based on the specific relationship and applicable law.