

Business Associate Agreement (BAA) Essentials

A plain-language reference for medical practices reviewing vendor BAAs.

When to use this guide

Use this reference when a vendor will handle protected health information (PHI) on behalf of your practice and you are reviewing the Business Associate Agreement (BAA) for that relationship.

It shows the main topics to look for. It is not model contract language and does not replace legal review

What a BAA should cover:

1. What a vendor may do with PHI

The agreement should state when the vendor is allowed or required to use or share PHI for the service.

2. What the vendor may not do

The vendor should agree not to use or share PHI for other purposes unless the agreement or law allows or requires it.

3. How PHI will be protected

The vendor should use appropriate safeguards and comply with the HIPAA Security Rule requirements that apply to electronic PHI.

4. When the vendor must tell you about problems

The agreement should require the vendor to report uses or sharing of PHI that the agreement does not allow, breaches of unsecured PHI, and security incidents. It may also define how routine unsuccessful attempts are handled.

5. Help with patient rights

If the vendor holds information needed to meet a patient's HIPAA rights, it should help your practice provide access to PHI, support required amendments, and provide information needed for an accounting of disclosures (a record of certain disclosures) when required.

6. HIPAA duties the vendor performs for your practice

If the vendor carries out a Privacy Rule obligation on your behalf, the agreement should require it to follow the HIPAA requirements that apply to that work.

7. Access for HHS when required

The vendor should make relevant records and practices available to the U.S. Department of Health and Human Services (HHS) when needed for a HIPAA compliance review.

8. Rules for subcontractors

A subcontractor that handles PHI on the vendor's behalf should agree to follow the same applicable restrictions and requirements.

9. What happens to PHI when the relationship ends

When feasible, PHI should be returned or destroyed. If some PHI must be kept, the agreement should require continued protection and limit how it can be used or disclosed.

10. The right to end the agreement for a serious violation

The agreement should give your practice the right to end the agreement if the business associate seriously fails to meet an important part of it.

Other contract terms worth defining clearly

- A clear incident-notification deadline. For a breach of unsecured PHI, HIPAA requires notice promptly and no later than the deadline it sets (currently 60 days after discovery); your contract can require faster notice.
- How data can be exported and what transition help the vendor will provide.
- Service availability, support, escalation, backup, restoration testing, and recovery expectations.
- Where sensitive information may be stored or processed.
- Require notice when important subcontractors, hosting providers, or the security model materially change.
- Which security responsibilities belong to the vendor, your practice, or both.
- What security evidence, assessment information, or audit rights (your ability to review or request an independent check of their security) are reasonable for the risk of the service.
- How long data is kept, how it is deleted, and what may remain in backups or archives.

A signed BAA is not a security score.

A BAA creates important legal obligations, but it does not prove that the vendor has a strong cybersecurity program. Use the Vendor Cybersecurity & HIPAA Due-Diligence Questionnaire to evaluate the broader risk.

Official HHS references:

[HHS - Sample Business Associate Agreement Provisions](#)

[HHS - Business Associates](#)

Legal note: HHS states that its sample provisions address HIPAA requirements only. They may not, by themselves, create a binding contract under state law, and they do not replace consultation with a lawyer or negotiations between the parties.