Business Associate Agreement (BAA) Basics

Understanding BAAs and when you need them

What is a Business Associate?

A business associate is a person or entity that performs certain functions or activities on behalf of, or provides services to, a covered entity that involve access to protected health information (PHI).

When Do You Need a BAA?

You need a BAA when:

- [ ] Your vendor will have access to PHI
- [ ] Your vendor creates, receives, maintains, or transmits PHI on your behalf
- [ ] Your vendor provides services that involve PHI (hosting, data processing, etc.)

Key Components of a BAA

- [ ] Permitted uses and disclosures of PHI
- [ ] Prohibition on unauthorized use or disclosure
- [ ] Safeguards to protect PHI
- [ ] Reporting requirements for breaches
- [ ] Subcontractor agreements
- [ ] Access to PHI for covered entity
- [ ] Return or destruction of PHI at termination
- [ ] Liability and indemnification clauses

Common Mistakes to Avoid

Not getting a BAA signed before PHI access: Always execute the BAA before any PHI is shared.

Using generic contracts: Ensure your BAA specifically addresses HIPAA requirements.

Forgetting about subcontractors: Your business associates must also have BAAs with their subcontractors.

Not reviewing BAAs regularly: Review and update BAAs annually or when regulations change.

BAA Checklist

- [ ] Identify all vendors with PHI access
- [ ] Request BAA from each vendor
- [ ] Review BAA for HIPAA compliance
- [ ] Have legal counsel review if needed
- [ ]

- Execute BAA before PHI sharing begins
- [ ] Maintain signed BAAs for 6 years
- [ ] Monitor vendor compliance